Handboek

Aansluiting van het schoolnetwerk op kennisnet

Deel 0: Inhoudsopgave en Voorwoord

Inhoudsopgave

Deel III: Software-instellingen

Indeling van deel III

Deel V: Geavanceerde instellingen

Indeling van deel V

Deel VI: Beveiliging en veiligheidsmaatregelen

Indeling van deel VI

Deel VII: Veelvoorkomende vragen

Indeling van deel VII

Colofon

Het 'Handboek kennisnet' ('Het Handboek') is een uitgave van nl.tree. Het Handboek wordt regelmatig herzien naar aanleiding van vragen van gebruikers van kennisnet, wijzigingen in het netwerk of de introductie van nieuwe diensten.

Redactie

Adres:

nl.tree
t.a.v. Redactie Het Handboek

Postbus 82097
2508 EB Den Haag
tel.: (070) 8900000
fax: (070) 8900099
e-mail: handboek@kennisnet.nl

Met dank aan

De redactie wil Jeroen Oldenhof (Systeembeheerder Drenthecollege) en Harry Spek (ICT-coördinator Calscollege Nieuwegein) speciaal bedanken voor hun bijdragen aan de totstandkoming van dit 'Handboek kennisnet'.

Voorwoord

In het Handboek kennisnet ('Het Handboek') wordt een aantal veelvoorkomende vragen en de antwoorden daarop uitgewerkt. Deze vragen zijn voortgekomen uit gesprekken met ICT-coördinatoren, gebruikers en het Ministerie van Onderwijs, Cultuur en Wetenschappen. Getracht is om de uitleg in het document zo levendig mogelijk te brengen en zaken zó uit te leggen, dat ook personen met slechts geringe ervaring met computers aan de hand van dit document aan de slag kunnen.

Het Handboek is slechts bedoeld als een informatief document; het bevat geen uitgebreid overzicht van de diensten van kennisnet. De exacte beschrijvingen van de geboden diensten kunt u terugvinden in de productbeschrijvingen. Afbeeldingen dienen slechts als illustratie, de tekst in Het Handboek is hierbij leidend. **Aan dit document kunnen géén rechten worden ontleend!**

Het Handboek wordt beschouwd als een 'levend' document, daar het regelmatig zal worden onderhouden en bijgewerkt. Indien u op- of aanmerkingen of suggesties heeft, kunt u deze doorgeven aan de redactie van Het Handboek via handboek@kennisnet.nl. Nieuwe versies van Het Handboek zullen op elektronische wijze beschikbaar worden gesteld via de website van kennisnet: http://www.kennisnet.nl/, onder 'Servicepunt'.

Met ingang van versie 2.0 is het document opgedeeld in een achttal afzonderlijke delen. Dit is gedaan om de onderhoudbaarheid van het document te verbeteren. Ook kunt u zelf beter kiezen welke delen voor u relevant zijn om te verversen.

De verschillende soorten software die in het handboek worden genoemd, dienen slechts als voorbeeld en zijn geen verplichting. Instellingen zijn te allen tijde vrij in hun keuze van bepaalde software. De portal http://software.pagina.nl kunt u gebruiken voor het vinden van software, freeware en shareware.

Servicepunt Kennisnet

Het Servicepunt Kennisnet is dé vraagbaak voor ICT-coördinatoren en andere geïnteresseerden over de aansluiting van scholen op kennisnet en het gebruik van kennisnetdiensten. Het Servicepunt is een gezamenlijk initiatief van bureau kennisnet.nl, nl.tree en het Cfi.

De belangrijkste verschijningsvorm van het Servicepunt is de website op het adres http://servicepunt.kennisnet.nl. Op deze website vindt men, naast het laatste nieuws over bijvoorbeeld storingen, onderhoudswerkzaamheden of wijzigingen in de regelgeving, uitgebreide informatie over het gehele proces van de aansluiting, het Handboek kennisnet, alle benodigde formulieren en officiële documenten, en een regelmatig bijgewerkt lijst met Veel Gestelde Vragen.

De lijst met veel gestelde vragen wordt in regelmatig onderling overleg bijgewerkt door de verantwoordelijke afdelingen binnen nl.tree, het Cfi en de redactie van bureau kennisnet. Alle scholen ontvangen van nl.tree een pakket met basisinformatie. Ook na het lezen hiervan kunnen er bij de ICT-coördinatoren nog allerlei vragen leven over kennisnet. Deze lijst probeert daar zoveel mogelijk een antwoord op te geven. De lijst kan doorzocht worden op onderwerp, maar ook op trefwoorden. De lijst behandelt alle aspecten van kennisnet: overeenkomsten, financiering en beleid; het proces van aansluiten; het gebruik van diensten en producten.

Mocht er onverhoopt geen passend antwoord gevonden kunnen worden op de Servicepunt website, dan is het altijd mogelijk om een e-mail te sturen naar: servicepunt@kennisnet.nl. Men krijgt dan zo spoedig mogelijk antwoord.

Voor dringende vragen is het ook mogelijk telefonisch contact op te nemen met de Service Desk op het speciale gratis telefoonnummer 0800-KENNISNET (0800-536647638). Men kan daarbij kiezen uit de volgende opties: (1) Beleidsvragen; (2) Technische vragen; (3) Storingsmeldingen. De Servicedesk is telefonisch bereikbaar van 07:00 uur tot 23:00 uur.

Opmerkingen en tips over de Servicepunt website kunt u mailen naar:
webmaster@servicepunt.kennisnet.nl.

Handboek

Aansluiting van het schoolnetwerk op kennisnet

Deel I: Opbouw kennisnet

Indeling van deel I

Hoofdstuk 1 vertelt wat kennisnet is. De basisdiensten van kennisnet komen globaal aan de orde.

Hoofdstuk 2 gaat over de structuur van het netwerk van kennisnet. De basisbegrippen van internet en kennisnet worden nader toegelicht. De hoofdlijnen van de netwerkstructuur worden uiteengezet.

1. Kennisnet

Dit hoofdstuk geeft een korte beschrijving van kennisnet. Hierin wordt verteld wat kennisnet is en welke basisdiensten kennisnet biedt en hoe kennisnet in grote lijnen werkt.

1.1 Wat is kennisnet?

Kennisnet is een beveiligd netwerk dat scholen en onderwijsinstellingen, musea en bibliotheken met elkaar verbindt. Met behulp van een internetverbinding en in een veilige, besloten omgeving, heeft de gebruiker van kennisnet toegang tot een enorme hoeveelheid educatieve informatie. Kennisnet is een initiatief van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het doel van kennisnet is het realiseren van een groot landelijk computernetwerk, waarop alle lagere en middelbare scholen en diverse andere onderwijs- en educatieve instellingen zijn aangesloten. Via dit netwerk kunnen de gebruikers de beschikbare kennis delen. Kennisnet wordt dus voor een belangrijk deel gemaakt en gevormd door de gebruikers zelf.

1.2 De basisdiensten van kennisnet

Als u een aansluiting hebt op kennisnet, kunt u van diverse diensten gebruikmaken. Deze diensten maken het mogelijk dat u kunt surfen op het internet, e-mailen met kennisnet- en internetgebruikers, chatten en deelnemen aan discussiegroepen die speciaal voor het onderwijs zijn geselecteerd. In onderstaande paragrafen lichten we de basisdiensten van kennisnet kort toe.

1.2.1 Toegang tot internet

Elke gebruiker heeft via kennisnet toegang tot het Internet en daarmee tot oneindig veel informatie, diensten en toepassingen. Deze internettoegang is niet beperkt in tijd; wie dat wil, kan 24 uur per dag van het internet gebruikmaken. Wel kunnen er beperkingen zijn in de informatie en de toepassingen die een gebruiker kan benaderen. Met behulp van filterprofielen kan de toegang tot bepaalde websites worden ontzegd, bijvoorbeeld racistische websites, websites voor volwassenen, toepassingen waarmee gebruikers kunnen gokken, etcetera. Deze filterprofielen worden ontwikkeld en geleverd door nl.tree.

1.2.2 E-mail

Elke gebruiker van kennisnet krijgt een eigen e-mailadres. Vanaf elke locatie kunnen gebruikers hun kennisnet-mail lezen, schrijven en verzenden. Deze toepassing heet webmail. De omvang van een e-mailbericht is beperkt tot 3 MB (megabyte).

1.2.3 Eigen domeinnaam

Elke school of instelling die zich aansluit op kennisnet en kiest voor de basisdiensten, krijgt een eigen domeinnaam. Deze domeinnaam heeft de volgende structuur:

www.[naam school/instelling].[plaatsnaam].kennisnet.nl

Als uw school of instelling al een eigen domeinnaam heeft, kunt u deze naam verplaatsen naar kennisnet. Ook kunt u desgewenst een eigen domeinnaam aanvragen, bijvoorbeeld een naam die korter is dan de naam die kennisnet u biedt. Daaraan zijn wel kosten verbonden. Zowel voor het behoud als voor de aanvraag van uw domeinnaam moet u contact opnemen met nl.tree.

1.2.4 Eigen website (webhotel)

Elke school kan een eigen website plaatsen op de server van kennisnet, het zogenoemde kennisnet Webhotel. Standaard krijgt elke school 5 MB schijfruimte op de server. Deze ruimte kan desgewenst worden uitgebreid met eenheden van 50 MB. We benadrukken dat de school zelf deze website moet bouwen, vullen en onderhouden. Dat is de essentie van kennisnet. De gebruikers bepalen de inhoud van kennisnet. De website is bereikbaar onder de domeinnaam van de school of instelling. Als uw school al een eigen domeinnaam heeft, kan het webhotel gebruikers verwijzen naar die domeinnaam.

Meer over het beheren van de website met kennisnet Webhotel leest u in deel IV.

1.2.5 Nieuwsgroepen

Met de dienst 'news' heeft de gebruiker van kennisnet toegang tot een wereldwijd netwerk van nieuwsgroepen, een soort elektronisch prikbord. De nieuwsgroepen zijn gerangschikt naar onderwerp. Elke gebruiker kan in zo'n nieuwsgroep een bericht plaatsen, waarop anderen kunnen reageren. De onderwerpen van de nieuwsgroepen zijn voornamelijk gerelateerd aan het onderwijs. Er is een scheiding tussen publieke nieuwsgroepen en interne kennisnetnieuwsgroepen. De nieuwsgroepen van kennisnet zijn alleen te benaderen door gebruikers van kennisnet.Voor het opnemen en doorgeven van publieke nieuwsgroepen is toestemming nodig van het Ministerie van Onderwijs, Cultuur en Wetenschappen.

1.3 Dus: gebruikers maken het kennisnet!

Zoals we eerder al schreven, wordt de inhoud van kennisnet bepaald door de gebruikers. Bijdragen van uw school of instelling geven vorm aan kennisnet. Dat kunnen bijdragen zijn van de leerlingen en de docenten maar ook van managers, ouders of anderen die bij het onderwijs zijn betrokken. Gebruik kennisnet dus niet alleen om informatie te zoeken, maar gebruik het vooral ook om informatie beschikbaar te stellen. Maak daarom een website van uw school of instelling en ga na wat u anderen wilt vertellen en wat u van anderen wilt weten:

- Vertel met welke projecten de school zich bezighoudt.
- Zet werkstukken op de website.
- Geef verdiepende informatie over examenstof.
- Toon de creatieve resultaten van handvaardigheidlessen.
- Wissel ideeën uit over onderwijsmethoden.
- Doe on-line een toets of een cursus.
- Doe suggesties voor boekenlijsten.
- Meld u aan bij een vakcommunity en leg contact met collega's elders in het land.
- Plaats een vacature.
- Discussieer in nieuwsgroepen over actuele zaken.
- Enzovoorts, enzovoorts

Kennisnet wordt pas echt een succes als u een bijdrage levert.

2. Basisbegrippen en structuur van kennisnet

In dit hoofdstuk leest u over de basisbegrippen en hoe de technische structuur van het landelijke netwerk van het kennisnet eruit ziet. Hierbij komen zaken als de 'backbone' (Nederlands: ruggengraat), het serverpark en de proxy-servers aan bod.

2.1 Basisbegrippen van kennisnet

Kennisnet werkt op basis van de technologie die ook wordt gebruikt op het wereldwijde internet. Het verschil is dat kennisnet een gesloten netwerk is dat via een zogenoemde firewall op een veilige manier toegang biedt tot de informatie die op het internet beschikbaar is. In deel III leest u meer over firewalls. Meer over de beveiliging van kennisnet leest u in deel VI van het handboek.

2.1.1 Internet-Protocol (IP)

Het internet is een wereldwijde verzameling van computers die via kabels of per satelliet met elkaar zijn verbonden. Al deze computers kunnen met elkaar communiceren op basis van een taal ('protocol') die IP heet: het internet Protocol. Kennisnet werkt op een vergelijkbare wijze. Zo kunnen scholen of andere aangesloten instellingen per computer met elkaar communiceren.

2.1.2 Routers

De communicatie tussen gebruikers van het kennisnet gaat niet rechtstreeks maar via 'routers'. Routers zijn speciale computers die ervoor zorgen dat IP-informatie de goede kant op gaat. Op het internet en dus ook op kennisnet bestaan vele kruispunten van verbindingen. Op die kruispunten staan routers, die de weg weten op het netwerk. Ook de kennisnet-schoolrouter is zo'n router. De kennisnet-schoolrouter ziet of de IP-informatie die op het netwerk van de school langskomt, bedoeld is voor de school intern of voor daarbuiten (kennisnet of elders in de wereld). Als het een interne stroom is, laat hij de informatie ongemoeid. Als het voor buiten is, stuurt hij de IP-stroom het kennisnet op, waar een stelsel van grotere routers ervoor zorgt dat de informatie op de plaats van bestemming komt: een andere school, een website of waar dan ook.

2.1.3 Informatiestromen

De internettaal IP knipt alle informatiestromen in stukjes en verstuurt deze als informatiepakketjes. Die IP-pakketjes zijn maximaal zo'n 1000 tekens groot (een vol A4tje is ongeveer het viervoudige daarvan) en bewegen zich geheel zelfstandig over het netwerk. Dat kan, omdat elk pakketje is voorzien van een bestemmingsadres ('dest-address'). De router leest dat 'dest-address' en weet dan waar hij het pakketje naartoe moet sturen. Elk IP-pakketje heeft ook een afzender, het 'source-address'. Hierdoor is altijd te zien waarvandaan de informatie is verstuurd. Dat maakt tweerichtingscommunicatie extra eenvoudig. In tegenstelling tot gewone post, is het bij het internet Protocol niet mogelijk het afzenderadres achterwege te laten.

2.1.4 IP-adressen

Om het internet (en ook kennisnet) te laten functioneren, moet elke computer een uniek adres hebben, anders is het niet mogelijk de informatie op de juiste plaats te krijgen. Dit unieke adres heet het IP-adres. Overigens hebben niet alleen computers maar ook routers een IP-adres. Zo'n IP-adres heeft de opbouw '`a.b.c.d`', waarbij a t/m d getallen zijn van 0 tot 255. Een voorbeeld van een IP-adres is `192.87.13.88`. Voor een netwerk zijn meerdere IP-adressen nodig, omdat elke computer in het netwerk een IP-adres nodig heeft. Zo'n reeks van IP-adressen is een IP-adresreeks.

Voor de distributie van IP-adressen is er een wereldwijd systeem van IP-nummeruitreiking. Als een instelling IP-nummers voor haar pc's wil, krijgt zij van haar Internet Service Provider (ISP), bijvoorbeeld kennisnet, een reeks IP-nummers. Dat kan een reeks van acht nummers zijn, maar ook van 64 of 1024, afhankelijk van de (aantoonbare) behoefte van de instelling.

Deze IP-nummers kunt u vervolgens automatisch of met de hand aan een computer toekennen. In deel III van het Handboek wordt precies uitgelegd hoe u dit moet doen.

In bijlage D in deel VII leest u meer over de indeling en opbouw van IP-adressen en IP-adresreeksen.

2.1.5 Indeling IP-reeks

Alle schoolrouters worden voorzien van filters. Deze filters delen de IP-reeks van uw schoolnetwerk in de volgende stukken:

- de router;
- één gereserveerd adres;
- werkplekken;
- lokale servers die op kennisnet 'zichtbaar' moeten zijn;
- lokale servers die *niet* op kennisnet 'zichtbaar' moeten zijn en overige netwerkapparatuur (hubs, routers, switches).

De indeling van de IP-adressen is voor *alle* kabelmaatschappijen en Energis gestandaardiseerd.

In bijlage D van deel VII leest u meer over de indeling en opbouw van IP-adressen en IP-adresreeksen.

2.1.6 Domeinnamen

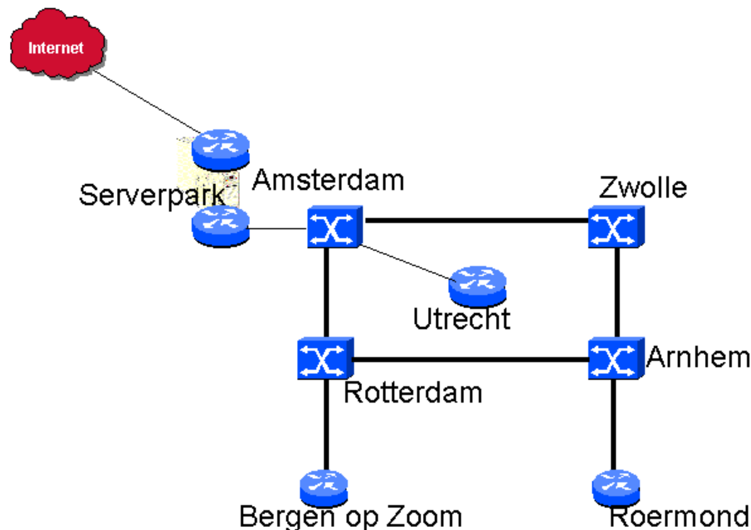
Als gebruiker is het niet nodig om IP-nummers uit het hoofd te leren. De domeinnaam kennen is voldoende. Een website met als domeinnaam bijvoorbeeld www.kennisnet.nl is immers veel makkelijker te onthouden dan een IP-nummer van mogelijk twaalf cijfers. Het Domain Name Service (DNS) zorgt ervoor dat een (domein)naam wordt vertaald naar het bijbehorende IP-nummer: in dit voorbeeld het IP-adres van de website van kennisnet. Vervolgens gebruikt de bewuste toepassing alleen nog maar het IP-nummer. De naam is alleen bedoeld voor communicatie met de gebruiker.

De extensie van een domeinnaam geeft informatie over de website. Zo staat "`.nl`" voor domeinnamen in Nederland, "`.de`" voor Duitsland, "`.be`" voor België, "`.com`" voor bedrijven internationaal, "`.edu`" voor onderwijsinstellingen in de Verenigde Staten, enzovoorts. De bijzondere positie die de Verenigde Staten met `.edu` (en ook met bijvoorbeeld `.mil` voor Amerikaanse militaire instanties) inneemt, is overigens een erfenis van de Amerikaanse oorsprong van het internet.

De informatie voor alle domeinnamen met de extensie `.nl` wordt bijgehouden door een instantie in Nederland (de Stichting Internet Domeinregistratie Nederland) die precies weet waar de DNS-informatie te vinden is voor de domeinen als `dsm.nl`, `kennisnet.nl`, `minocw.nl`, `philips.nl`. Zo zijn er vergelijkbare instanties die de informatie bijhouden voor `.de`, `.com`, `.be`, `.edu`, `.mil`, enzovoorts.

2.2 De backbone van kennisnet

Het hoofdonderdeel van het netwerk is de 'backbone', de ruggengraat. Deze backbone bestaat uit verbindingen tussen Amsterdam, Rotterdam, Zwolle en Arnhem, en verzorgt de communicatie tussen de netwerken van regionale kabelmaatschappijen en het serverpark.



Figuur 1: 'Backbone' van kennisnet met de belangrijkste verbindingen

In Figuur 1 is een schematische afbeelding van de backbone van kennisnet weergegeven. De blauwe vierkante objecten zijn zogenoemde ATM-switches. Een van de taken van de ATM-switches is de capaciteit van het netwerk te verdelen op basis van de behoefte aan capaciteit. De blauwe ronde objecten zijn hoofdrouters van kennisnet, waaraan belangrijke netwerkonderdelen van onder andere de regionale kabelmaatschappijen zijn gekoppeld.

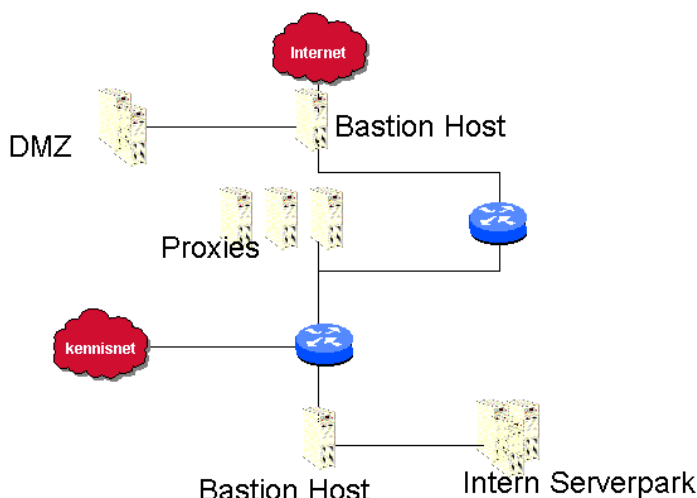
Tussen het serverpark en elk zogenoemd uitkoppelpunt (de plaats waar de kabelmaatschappij haar netwerk koppelt aan de backbone) zijn twee virtuele verbindingen gemaakt. Verkeer vanaf een schoollocatie naar het serverpark kan zo via twee verschillende (virtuele) routes over de backbone zijn bestemming bereiken.

2.3 Het serverpark van kennisnet

Het serverpark van kennisnet is de plaats waar alle diensten zijn ondergebracht die kennisnet aanbiedt aan de gebruikers. Er staan grote computersystemen (servers) die belangrijke taken uitvoeren om kennisnet naar behoren te laten functioneren.

Hoewel fysiek alles op dezelfde locatie staat, is het serverpark in drie delen op te splitsen:

- het interne serverpark;
- het externe serverpark (DMZ);
- de proxy -servers (proxies).



Figuur 2: Schematische weergave van het serverpark

Naast de genoemde onderdelen zijn er 'bastion hosts' aanwezig. Dit zijn systemen die het netwerkverkeer controleren en bepalen of dat mag worden doorgelaten of niet. Het systeem van een bastion host, proxy-servers en een 'demilitarized zone' wordt ook wel 'firewall' genoemd.

2.3.1 Het interne serverpark

In het interne serverpark staan de meeste computersystemen (servers), die diensten aanbieden aan de gebruikers van kennisnet. Hierbij kunt u denken aan de mail- en newsservers, een interne webserver en de centrale DHCP- en DNS-servers.

Deze servers hebben *geen* rechtstreeks contact met de buitenwereld en zijn niet rechtstreeks van buiten kennisnet te benaderen. Dit is zo gemaakt om kennisnet en de vitale systemen optimaal te kunnen beschermen. Als deze servers moeten communiceren met de buitenwereld (bijvoorbeeld bij uitwisseling van e-mailberichten), gebeurt dat *altijd* via de servers van het externe serverpark.

2.3.2 Het externe serverpark (DMZ)

In het externe serverpark, ook wel DMZ (Demilitarized Zone) genoemd, staan de computersystemen die een belangrijk deel van de communicatie met de buitenwereld verzorgen. Zo staan hier de webservers van kennisnet en de DNS-servers die ervoor zorgen dat de systemen van kennisnet (en van de scholen) op het internet te vinden zijn. Ook staan hier computersystemen die e-mail en news doorsturen van het internet naar kennisnet en andersom. Deze systemen worden ook wel 'relay-servers' genoemd.

2.3.3 De proxy-servers

Het woord 'proxy' betekent 'gevolmachtigde' of 'vertegenwoordiger'. Een proxy verricht dus namens u een handeling. Een proxy-server is een server die taken voor u verricht, zoals het ophalen van gegevens vanaf het internet of het maken van een verbinding met een systeem op het internet. Deze servers zijn de enige computers die rechtstreeks mogen communiceren met de buitenwereld en zij vormen ook de scheiding tussen de 'binnenkant' en de 'buitenkant' van het netwerk van kennisnet. Er is dus geen rechtstreeks verkeer van binnen naar buiten, of andersom.

Door deze beveiligingsmaatregelen is het in principe niet mogelijk dat iemand vanaf het internet rechtstreeks uw systemen of de interne systemen van kennisnet benadert.

Handbook

Aansluiting van het schoolnetwerk op kennisnet

Deel II: Fysieke aansluiting

Indeling van deel II

Hoofdstuk 3 gaat over de fysieke aansluiting van een individuele computer of een netwerk op kennisnet.

3. Fysieke aansluiting

In dit hoofdstuk leest u hoe u een individuele computer en/of het lokale netwerk van uw organisatie kunt aansluiten op kennisnet.

3.1 Benodigde elementen

Voor het aansluiten van uw netwerk op kennisnet hebt u het volgende nodig:

- Een zogenoemd RJ45-stopcontact. We gaan ervan uit dat bij uw organisatie een RJ45-stopcontact is aangebracht door uw kabelmaatschappij, regionaal telecommunicatiebedrijf (RTB) of Energis (ISDN, VPoP en huurlijnen).
- Een standaard ethernetkabel met RJ45-stekkers (zie Figuur 3), voor het koppelen van een netwerk aan kennisnet (zie paragraaf 3.4.1). Gebruik altijd standaard ethernetkabels van categorie 5. Dergelijke bekabeling is toekomstvast. Zorg dat de kabels niet langer zijn dan tien meter om storingen in het netwerkverkeer te voorkomen.



Figuur 3: RJ45-bekabeling voor ethernet met RJ45-stekkers[1] (categorie 5)

- Een gekruiste ethernetkabel (kruiskabel) met RJ45-stekkers. U kunt een individuele computer met een gekruiste ethernetkabel op kennisnet aansluiten (zie paragraaf 3.3). Ook een netwerk aansluiten is ermee mogelijk, mits de hub een kruispoort heeft (zie paragraaf 3.4.2).
- Een kabelmodem.
- Een router.
- Een ethernet-hub (zie Figuur 4). U hebt een ethernet-hub nodig als u een netwerk op kennisnet wilt aansluiten.



Figuur 4: Ethernet-hub[2]

3.2 Verschil tussen standaard en gekruiste ethernetkabel

Voor ethernet, ook wel UTP-('Unshielded Twisted Pair'-)ethernet genoemd, kunnen ten minste twee soorten RJ45-kabels worden gebruikt. Voor kennisnet gaat het om standaard kabel en gekruiste kabel (kruiskabel).

---

[1] [Bron afbeelding: http://www.accesscomms.com.au/]

[2] [Bron afbeelding: http://www.netlux.com/]

Het is belangrijk dat u het verschil kunt bepalen. Soms hebt u daarvoor een vergrootglas nodig; dit is afhankelijk van de doorzichtigheid van het plastic van de RJ45-stekkers.

- Houd de twee kabeluiteinden met de RJ45-stekkers naast elkaar, zodat u de gekleurde draden kunt zien. Het beste zicht krijgt u meestal met het handeltje dat aan de stekkers zit naar beneden.

Wat is het verschil?

3.2.1 Standaard ethernetkabel

De gekleurde draden van standaard ethernetkabel, zoals zichtbaar in de RJ45-stekkers, hebben aan beide uiteinden van de kabel dezelfde volgorde.

3.2.2 Gekruiste ethernetkabel

De eerste (uiterst links) gekleurde draad aan het ene uiteinde van gekruiste ethernetkabel (kruiskabel), zoals zichtbaar in de ene RJ45-stekker, is de derde gekleurde draad aan het andere uiteinde van de kabel, zoals zichtbaar in de andere RJ45-stekker. Enkele gekleurde draden kruisen elkaar dus.

3.3 Aansluiten van een individuele computer op kennisnet

Een individuele computer kunt u op ethernet aansluiten met een gekruiste ethernetkabel (zie paragraaf 3.2). Als een los kabelmodem en een losse router zijn geleverd, moet u de gekruiste kabel koppelen aan de router.

Als u de kabel hebt aangesloten en beide apparaten hebt ingeschakeld, moet zowel op de kennisnetaansluiting als op de netwerkkaart van de computer een lampje branden. Als dat niet het geval is, moet u de volgende controles uitvoeren:

- Controleer of ondersteuning voor uw netwerkkaart op de desbetreffende PC is geïnstalleerd.
- Controleer of u de juiste kabel hebt gebruikt.

3.4 Aansluiten van een netwerk op kennisnet

Als u een netwerk wilt aansluiten op kennisnet moet u gebruikmaken van een of meer ethernet-hubs (zie Figuur 4). Een hub is een apparaat dat het netwerkverkeer distribueert. U kunt computers aan een ethernet-hub koppelen met standaard ethernetkabels (categorie 5, zie Figuur 3) of met gekruiste ethernetkabels (zie voor het verschil paragraaf 3.2). Een hub heeft een kruispoort of een poort die (door een schakelaar) als gewone en als kruispoort kan functioneren.

3.4.1 Aansluiting via een gewone poort

Als u uw aansluiting aan een gewone poort wilt koppelen, moet u een standaard ethernetkabel gebruiken (zie paragraaf 3.2).

Steek de ene stekker van de standaard ethernetkabel in de gewone poort van de hub en de andere stekker in de kennisnetaansluiting. Als de kabels correct zijn aangesloten en de apparaten zijn ingeschakeld, zal op de hub voor iedere aansluiting een lampje branden, evenals op de aangesloten apparatuur.

3.4.2 Aansluiting via een kruispoort

Als u uw aansluiting aan een kruispoort wilt koppelen, moet u een gekruiste ethernetkabel gebruiken (zie paragraaf 3.2).

Steek de ene stekker van de gekruiste kabel in de kruispoort van de hub en de andere stekker in de kennisnetaansluiting. Als de kabels correct zijn aangesloten en de apparaten zijn ingeschakeld, zal op de hub voor iedere aansluiting een lampje branden, evenals op de aangesloten apparatuur.

3.5 Aansluiten netwerk met BNC/AUI-kabels

Sommige lokale netwerken werken niet met UTP-ethernetkabels (dunne kabel met kleine RJ45-stekkers, zie Figuur 3 en paragraaf 3.2), maar met BNC-kabels (coaxkabels met een ronde bajonetsluiting), of AUI-kabels (coaxkabels met een D-vormige stekker). Zie Figuur 5 en Figuur 6.



Figuur 5: BNC[3]



Figuur 6: AUI[4]

De coaxsystemen maken gebruik van dezelfde ethernet-technologie als het UTP-ethernet-systeem. U kunt uw coaxnetwerk zonder probleem verbinden met de UTP-ethernet-aansluiting. U moet daarvoor wel een hub gebruiken waarop u zowel coax- als UTP-ethernetkabels kunt aansluiten. Als u zo'n hub aanschaft, moet u erop letten dat de hub de juiste aansluiting heeft (AUI of BNC) en of de hub in het netwerk kan worden geplaatst. Als u een 'fast ethernet'-netwerk hebt, kunt u het beste kiezen voor een 'dual speed'-hub voor 10 of 100 megabit per seconde (Mb/s).



Figuur 7: T-stuk BNC[5]

Als u een 'dual speed'-hub hebt en gebruikmaakt van AUI, hebt u ook een vrije 'transceiver' nodig. Deze transceiver verbindt u met een ethernet-AUI-kabel aan de hub. Als u een 'dual speed'-hub hebt en gebruikmaakt van BNC, moet u een extra BNC T-stuk aanbrengen in de bekabeling, zie Figuur 7. De poot van de 'T' moet u aansluiten op de BNC-ingang van de hub. Let altijd goed op of er zogenoemde 'male'- of 'female'-verbindingen worden gebruikt.

Als u de hub hebt aangesloten op het coaxnetwerk, moet u de hub vervolgens met een standaard UTP-ethernetkabel (dus géén gekruiste ethernetkabel, zie paragraaf 3.2) verbinden met de kennisnetaansluiting.

3.6 Problemen met de aansluiting

Als het lampje op de hub/switch of de netwerkkaart niet brandt, is de computer of het netwerk niet correct aangesloten op het kennisnet. Hieronder leest u een aantal mogelijke oorzaken en hoe u het desbetreffende probleem kunt oplossen.

- 10 Mb-ethernetkaarten

  Als u 10 Mb- ethernetkaarten gebruikt in combinatie met een 10/100 Mb-hub/-switch, kan dit de oorzaak zijn. Als u een andere hub (10 Mb) tussen de 10/100 Mb-hub en de PC plaatst, lost dit vaak het probleem op.

- Kabels

  De kabel is kapot of u gebruikt een gekruiste ethernetkabel in plaats van een standaard ethernetkabel, zie paragraaf 3.2 voor het verschil. Als u de juiste kabel gebruikt, moet het probleem zijn opgelost.

---

[3] [Bron afbeelding: http://www.net-shop.co.uk/productf/cacoaxef.htm]

[4] [Bron afbeelding: http://www.net-shop.co.uk/productf/cacoaxef.htm]

[5] [Bron afbeelding: http://bugs.wpi.edu:8080/EE535/hwk97/hwk5cd97/yqin/sc1.htm]

- Netwerkkaart wordt niet ondersteund

  De besturingssoftware van de PC ondersteunt de netwerkkaart niet. Controleer of u de juiste stuurprogramma's ('drivers') hebt geïnstalleerd en informeer of uw besturingssysteem de netwerkkaart ondersteunt.

- Uplink-poort

  Sommige hubs hebben een 'uplink-poort'. Deze fungeert als kruispoort, waarmee u verbindingen met andere hubs kunt realiseren. Op deze poort kunt u alleen met een gekruiste ethernetkabel een PC aansluiten. Sommige hubs hebben een knop om te schakelen tussen een normale poort en een kruispoort; soms is de poort dubbel uitgevoerd. In het laatste geval kunt u slechts één van beide poorten gebruiken, anders doen ze het geen van beide.

3.7 Verbetering performance

U moet altijd een hub of switch gebruiken om uw netwerk te koppelen aan de kennisnetrouter. Als uw hub rechtstreeks is aangesloten op de kennisnetrouter en als er veel lokaal verkeer is tussen uw werkstations en servers onderling, kan performanceverlies optreden. Dit kunt u verhelpen door een hub of switch te gebruiken die 100 Mb/s, of gemengd 10 Mb/s en 100 Mb/s aankan.

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel III: Software-instellingen

Indeling van deel III

In Hoofdstuk 4 nemen we onder de loep hoe u met Windows, Mac OS en andere besturingssystemen een verbinding met kennisnet kunt maken.

In Hoofdstuk 5 gaan we in op de kennisnetinstellingen voor webbrowsers, e-mail-programma's en andere applicaties waarmee u kunt werken op kennisnet.

Hoofdstuk 6 bevat een overzicht van de op kennisnet van toepassing zijnde netwerkadressen (IP-adressen).

Hoofdstuk 7 behandelt veelvoorkomende en belangrijke (fout)meldingen die kunnen voorkomen bij het gebruik van kennisnet en het internet.

4. Een verbinding met kennisnet maken: software-instellingen

Dit hoofdstuk geeft antwoord op de vraag hoe verschillende besturingssystemen kunnen worden ingesteld om gebruik te maken van kennisnet. In het vervolg van dit hoofdstuk maakt u voor elk van de besturingssystemen kennis met twee manieren om een verbinding met kennisnet te maken: dynamisch en statisch.

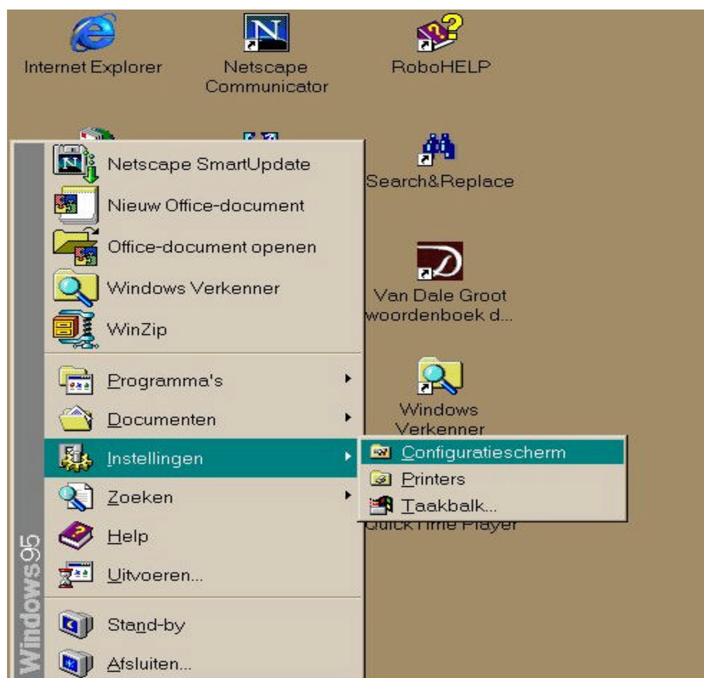
Let op!

Als in de loop van dit hoofdstuk wordt gesproken van het maken van een automatische verbinding met kennisnet, dan wordt een zogenoemde dynamische verbinding bedoeld. Wanneer wordt verwezen naar 'zelf de kennisnetinstellingen invoeren', dan wordt daarmee een statische verbinding bedoeld. Hoewel beide manieren om een verbinding met kennisnet te maken in technisch opzicht verschillen, merkt de gemiddelde gebruiker daar in de praktijk vrijwel niets van. Beginnende gebruikers wordt aangeraden om een dynamische (automatische) verbinding met kennisnet te maken. U hoeft slechts enkele instellingen zelf in te voeren. De overige instellingen worden automatisch toegewezen.

4.1 Hoe maak ik met Windows 95/98/NT4 een automatisch verbinding met kennisnet?

Volg de volgende procedure om een automatische (dynamische) verbinding met kennisnet te maken.

- Klik op de knop 'Start' op het bureaublad.
- Ga naar 'Instellingen' en vervolgens 'Configuratiescherm'.



Figuur 8: Bureaublad: Startmenu, Instellingen, Configuratiescherm

- Klik op 'Configuratiescherm'.

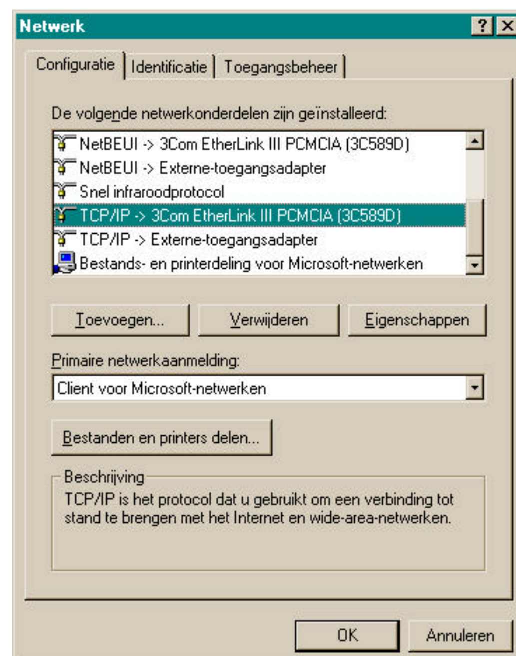
Het volgende scherm wordt geopend.



Figuur 9: Configuratiescherm

- Dubbelklik op het pictogram ‘Netwerk’.

Het scherm ‘Netwerk’ wordt geopend.

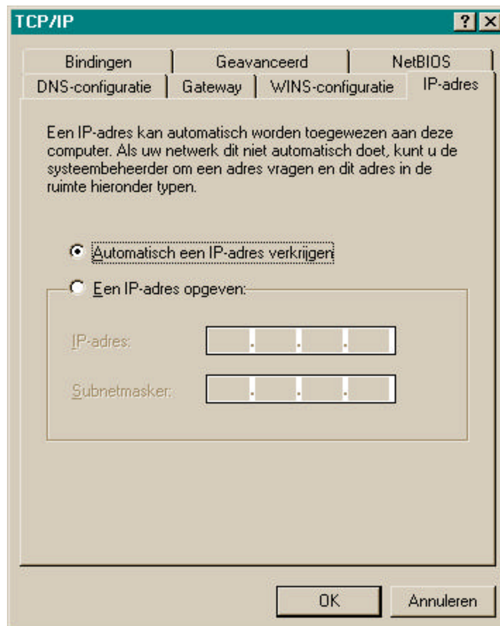


Figuur 10: Netwerk

Standaard wordt het tabblad ‘Configuratie’ geopend.

- Selecteer in de keuzelijst van het tabblad ‘Configuratie’ het netwerkonderdeel ‘TCP/IP→[*ethernetkaart*]’ (de *ethernetkaart* in bovenstaand voorbeeld is ‘3Com Etherlink III PMCIA (3C589D)’).
- Klik op de knop ‘Eigenschappen’.

Het scherm ‘TCP/IP’ wordt geopend. Standaard verschijnt het tabblad ‘IP-adres’.



Figuur 11: TCP/IP, IP-adres

- Selecteer het keuzerondje 'Automatisch een IP-adres verkrijgen'.
- Klik vervolgens op de knop 'OK' om de instellingen op te slaan.

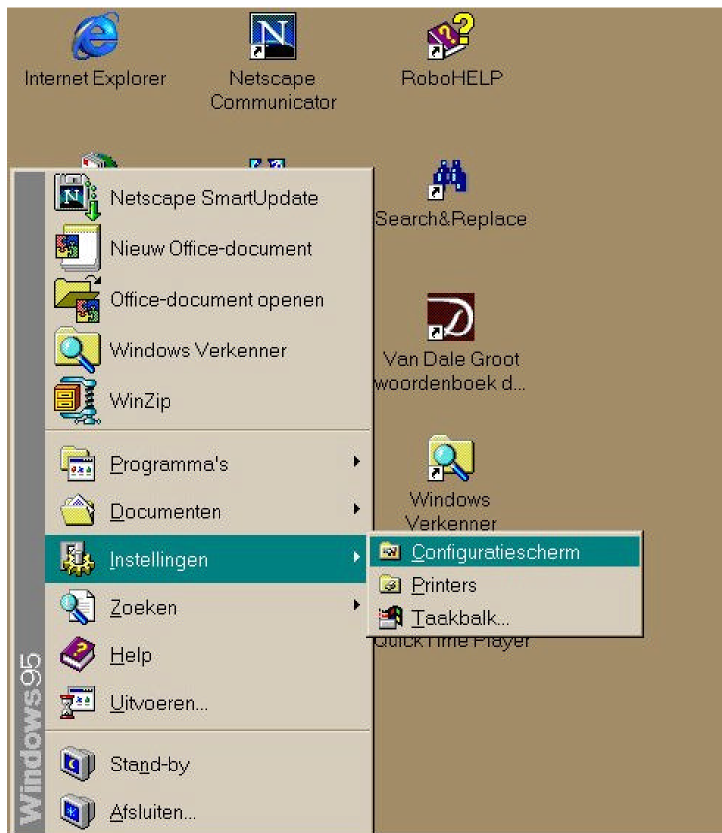
U hebt nu alle handelingen verricht om een automatische (dynamische) verbinding met kennisnet te maken.

Meer technisch betekent dit dat een op deze manier ingestelde pc automatisch een IP-adres zal aanvragen. De schoolrouter (het kennisnetmodem) vangt deze aanvraag op en zorgt ervoor dat de centrale DHCP-server een IP-nummer zal verstrekken dat binnen het aan de school toegekende bereik valt.

4.2 Hoe stel ik met Windows 95/98/NT zelf de kennisnetinstellingen in?

Volg de volgende procedure om zelf een verbinding met kennisnet te maken.

- Klik op de knop 'Start' op het bureaublad.
- Ga naar 'Instellingen' en vervolgens 'Configuratiescherm'.



Figuur 12: Bureaublad: Startmenu, Instellingen, Configuratiescherm

- Klik op ‘Configuratiescherm’.

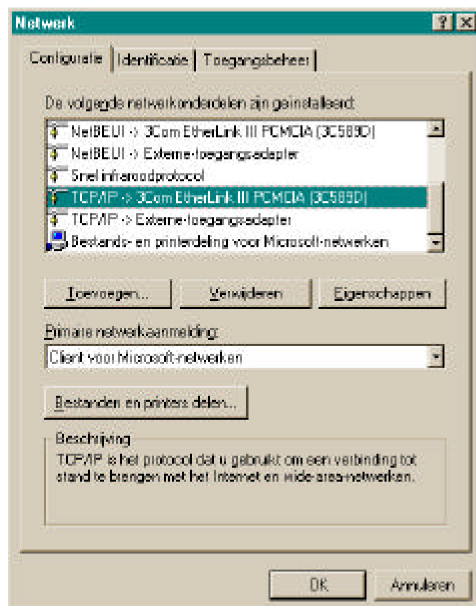
Het volgende scherm wordt geopend.



Figuur 13: Configuratiescherm

- Dubbelklik op het pictogram ‘Netwerk’.

Het scherm 'Netwerk' wordt geopend.

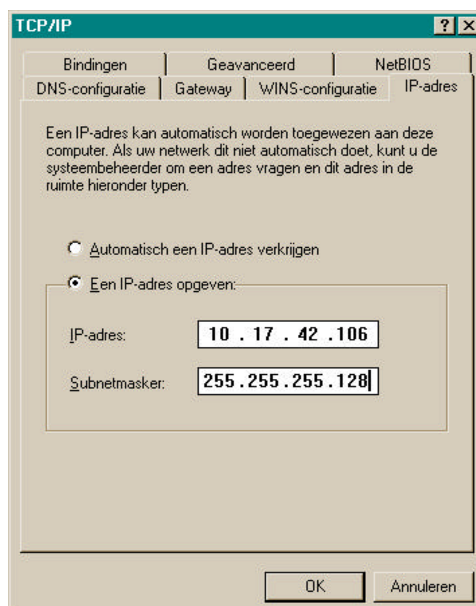


Figuur 14: Netwerk, Configuratie

Standaard wordt het tabblad 'Configuratie' geopend.

- Selecteer in de keuzelijst van het tabblad 'Configuratie' het netwerkonderdeel 'TCP/IP→[*ethernetkaart*]' (de *ethernetkaart* in bovenstaand voorbeeld is '3Com Etherlink III PMCIA (3C589D)').
- Klik op de knop 'Eigenschappen'.

Het scherm 'TCP/IP' wordt geopend. Standaard verschijnt het tabblad 'IP-adres'.



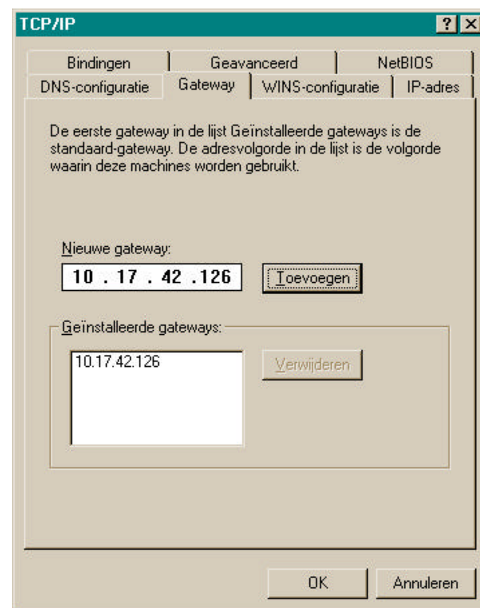
Figuur 15: TCP/IP, IP-adres

- Selecteer het keuzerondje ‘Een IP-adres opgeven’.
- Voer in het veld ‘IP-adres’ het vaste IP-adres van de pc in.
- Voer in het veld ‘Subnetmasker’ het subnetmasker in.

Deze gegevens zou u van uw kabelmaatschappij ontvangen moeten hebben (of van het bedrijf dat uw school op kennisnet heeft aangesloten). Wanneer u nog niet over deze gegevens beschikt, kunt u via het Servicepunt Kennisnet alsnog uw gegevens opvragen.

- Klik vervolgens op het tabblad ‘Gateway’.

Het volgende scherm wordt geopend.



Figuur 16: TCP/IP, Gateway

- Selecteer in het veld ‘Geïnstalleerde gateways’ de IP-adres(sen) van de gateway(s) die al geïnstalleerd zijn.

De knop verwijderen wordt actief.

- Klik op de knop verwijderen.

U hebt nu de bestaande gateway(s) verwijderd.

- Voer in het veld ‘Nieuwe gateway’ het IP-adres van de schoolrouter aan de kant van uw lokale netwerk (het kennisnetmodem) in.

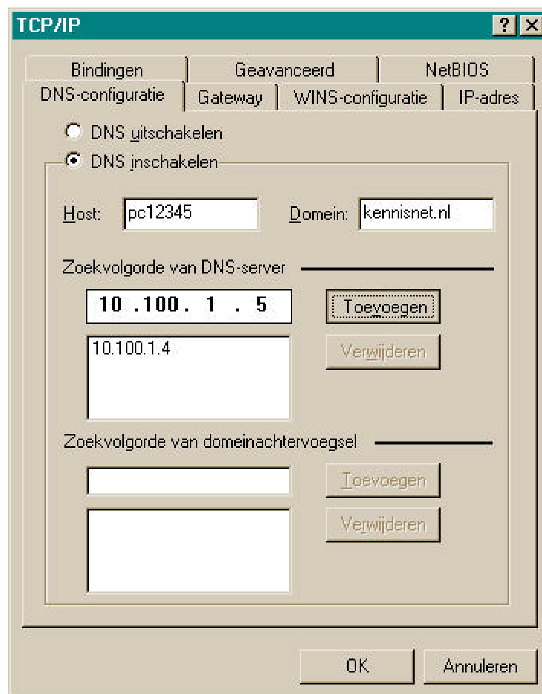
Dit is het hoogst of het laagst beschikbare IP-adres uit de aan u toegekende reeks adressen.

- Klik vervolgens op de knop ‘Toevoegen’.

Het door u ingevoerde IP-adres (gateway) verschijnt in het veld ‘Geïnstalleerde gateways’.

- Klik vervolgens op het tabblad ‘DNS-configuratie’

Het volgende scherm wordt geopend.



Figuur 17: TCP/IP, DNS-configuratie

- Selecteer het keuzerondje ‘DNS inschakelen’.

Een aantal velden wordt actief.

- Voer in het veld ‘Host’ de naam van de pc in.

In principe moet dit een unieke naam zijn. Bijvoorbeeld het BRIN- en vestigingsnummer van uw school, de aanduiding ‘pc’, gevolgd door een volgnummer, bijvoorbeeld: ‘`99ZZ99PC0023`’.

- Voer in het veld ‘Domein’ de domeinnaam van kennisnet in (‘`kennisnet.nl`’).

- Selecteer vervolgens de IP-adressen van de bestaande DNS-servers (deze staan in het grote veld onder het veld ‘Zoekvolgorde van DNS-server’).

De knop ‘Verwijderen’ wordt actief.

- Klik op de knop ‘Verwijderen’.

U hebt nu de IP-adressen van de bestaande DNS-server(s) verwijderd. Vervolgens voert u de DNS-servers van kennisnet in.

- Voer in het veld ‘Zoekvolgorde van DNS-server’ het IP-adres ‘`212.178.5.4`’ in.

- Klik op de knop ‘Toevoegen’.

Het IP-adres ‘`212.178.5.4`’ verschijnt in het grote veld onder het veld ‘Zoekvolgorde van DNS-server’.

- Voer vervolgens in het veld ‘Zoekvolgorde van DNS-server’ het IP-adres ‘`212.178.5.5`’ in.

- Klik op de knop ‘Toevoegen’.

Het IP-adres ‘`212.178.5.5`’ verschijnt in het grote veld onder het veld ‘Zoekvolgorde van DNS-server’.

- Klik op de knop ‘OK’ onderaan het scherm ‘TCP/IP’.

U hebt nu alle handelingen verricht om een verbinding met kennisnet te maken.

4.3 Windows 2000 en kennisnet

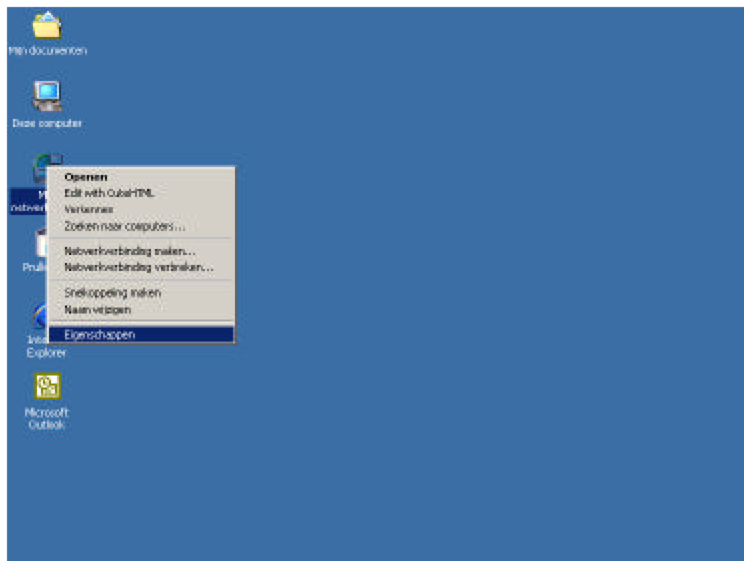
Ook met Windows 2000 kunt u een verbinding met kennisnet maken. Bovendien kunt u met de uitgebreide beheerfuncties in Windows 2000 Server, waaronder Terminal Services, WSH en MMC, servers, netwerken en pc's efficiënt beheren. Daarnaast biedt Windows 2000 de mogelijkheid om een eigen DNS-service op te zetten. Raadpleeg hiervoor de gebruikershandleiding die bij Windows 2000 is geleverd.

Hieronder nemen we het maken van een automatische verbinding met kennisnet onder de loep. Ook bekijken we hoe u zelf de kennisnetinstellingen kunt invoeren.

4.3.1 Hoe maak ik met Windows 2000 een automatische (dynamische) verbinding met kennisnet?

Volg de volgende procedure om een automatische verbinding met kennisnet te maken.

- Klik met de rechtermuisknop op het pictogram 'Mijn netwerklocatie'.
- Kies 'Eigenschappen'.



Figuur 18: Bureaublad, Mijn netwerklocatie, Eigenschappen

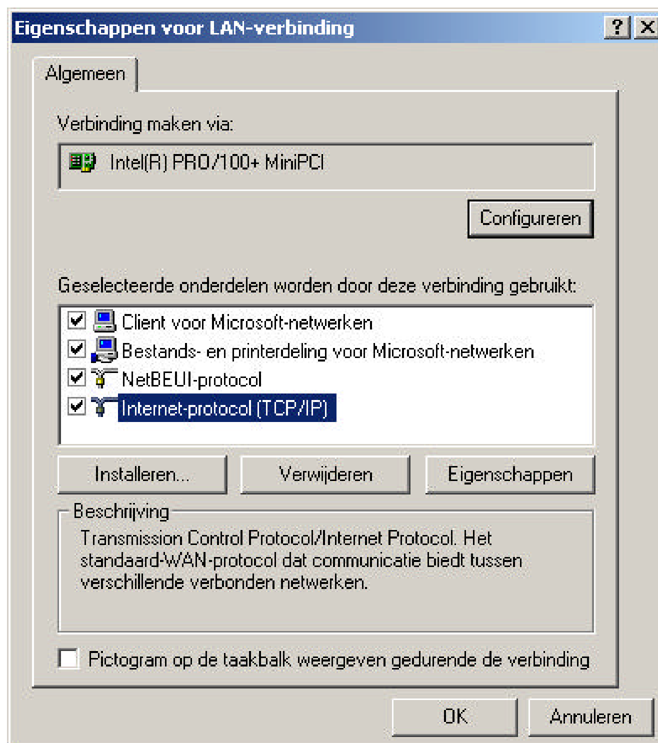
Het venster 'Netwerk- en inbelverbindingen' verschijnt.



Figuur 19: Netwerk- en inbelverbindingen

- Klik met de rechtermuisknop op het pictogram ‘LAN-verbinding’.
- Kies ‘Eigenschappen’.

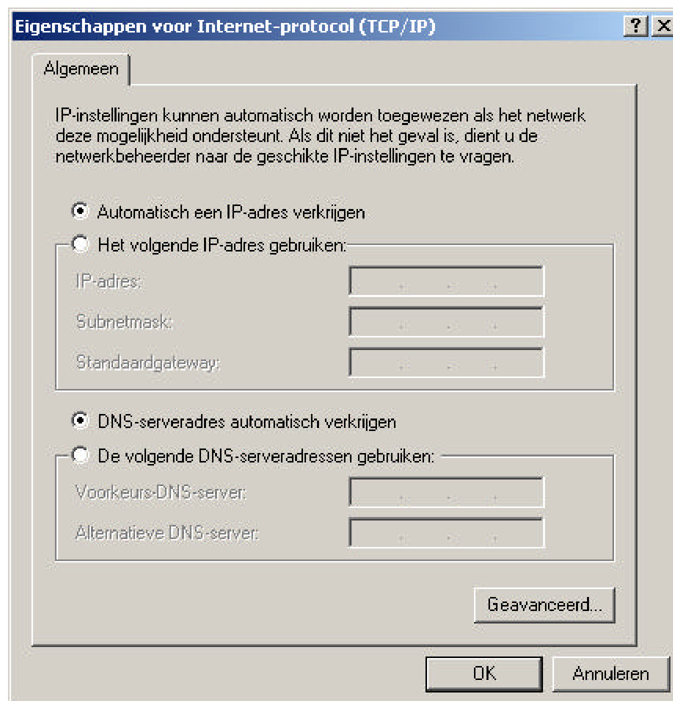
Het venster ‘Eigenschappen voor LAN-verbinding’ verschijnt.



Figuur 20: Eigenschappen voor LAN-verbinding, Algemeen

- Selecteer in de keuzelijst de optie ‘internet-protocol (TCP/IP)’.
- Klik op de knop ‘Eigenschappen’.

Het venster 'Eigenschappen voor internet-protocol (TCP/IP)' verschijnt.



Figuur 21: Eigenschappen voor internet-protocol (TCP/IP), Algemeen

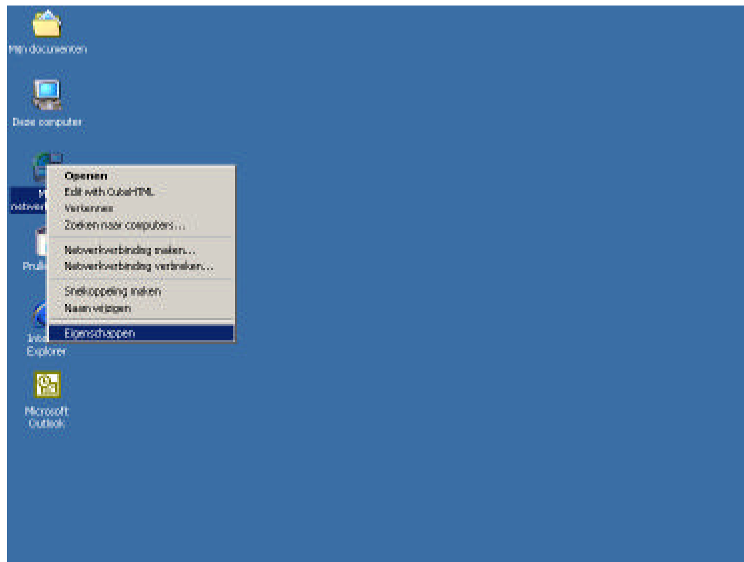
- Selecteer het keuzerondje 'Automatisch een IP-adres verkrijgen'.
- Selecteer het keuzerondje 'DNS-serveradres automatisch verkrijgen'.
- Klik op de knop 'OK' om de instellingen op te slaan en terug te keren naar het venster 'Eigenschappen voor LAN-verbinding'.
- Klik op de knop 'OK' om terug te keren naar het bureaublad.

U bent nu verbonden met kennisnet.

4.3.2 Hoe stel ik met Windows 2000 zelf de kennisnetinstellingen in?

Volg de volgende procedure om zelf een verbinding met kennisnet te maken.

- Klik met de rechtermuisknop op het pictogram 'Mijn netwerklocatie'.
- Kies 'Eigenschappen'.



Figuur 22: Bureaublad, Mijn netwerklocatie, Eigenschappen

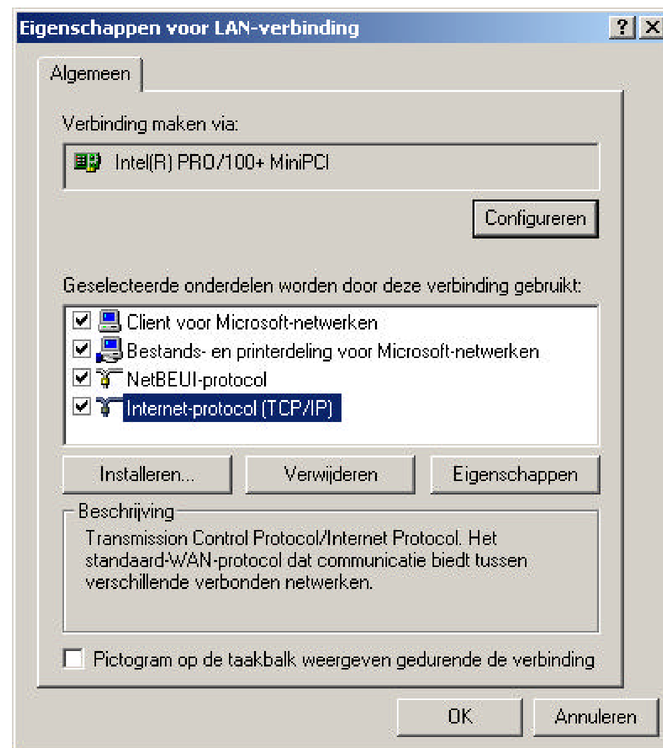
Het venster ‘Netwerk- en inbelverbindingen’ verschijnt.



Figuur 23: Netwerk- en inbelverbindingen

- Klik met de rechtermuisknop op het pictogram ‘LAN-verbinding’.
- Kies ‘Eigenschappen’.

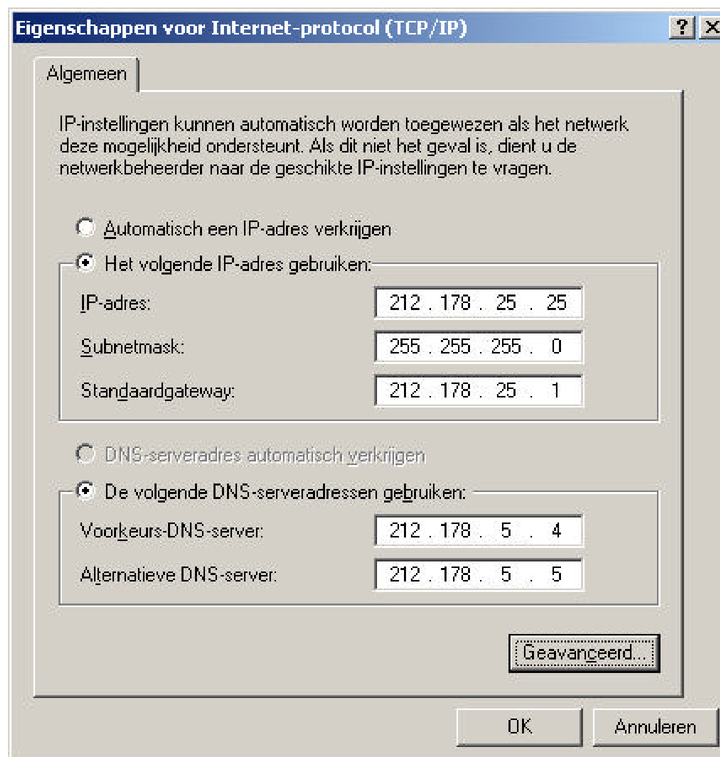
Het venster ‘Eigenschappen voor LAN-verbinding’ verschijnt.



Figuur 24: Eigenschappen voor LAN-verbinding, Algemeen

- Selecteer in de keuzelijst de optie ‘internet-protocol (TCP/IP)’.
- Klik op de knop ‘Eigenschappen’.

Het venster ‘Eigenschappen voor internet-protocol (TCP/IP)’ verschijnt.



Figuur 25: Eigenschappen voor internet-protocol (TCP/IP), Algemeen

- Selecteer het keuzerondje ‘Het volgende IP-adres gebruiken’.
- Voer in het veld ‘IP-adres’ het vaste IP-adres van de pc in.
- Voer in het veld ‘Subnetmask’ het subnetmasker in.
- Voer in het veld ‘Standaardgateway’ het IP-adres van de gateway in.

Deze gegevens ontvangt u van uw kabelmaatschappij (of van het bedrijf dat uw school op kennisnet heeft aangesloten). Wanneer u nog niet over deze gegevens beschikt, kunt u via het Servicepunt Kennisnet alsnog uw gegevens opvragen.

- Selecteer vervolgens het keuzerondje ‘De volgende DNS-serveradressen gebruiken’.
- Voer in het veld ‘Voorkeurs-DNS-server’ het IP-adres ‘`212.178.5.4`’ in.
- Voer in het veld ‘Alternatieve DNS-server’ het IP-adres ‘`212.178.5.5`’ in.
- Klik op de knop ‘OK’ om de instellingen op te slaan en terug te keren naar het venster ‘Eigenschappen voor LAN-verbinding’.
- Klik op de knop ‘OK’ om terug te keren naar het bureaublad.

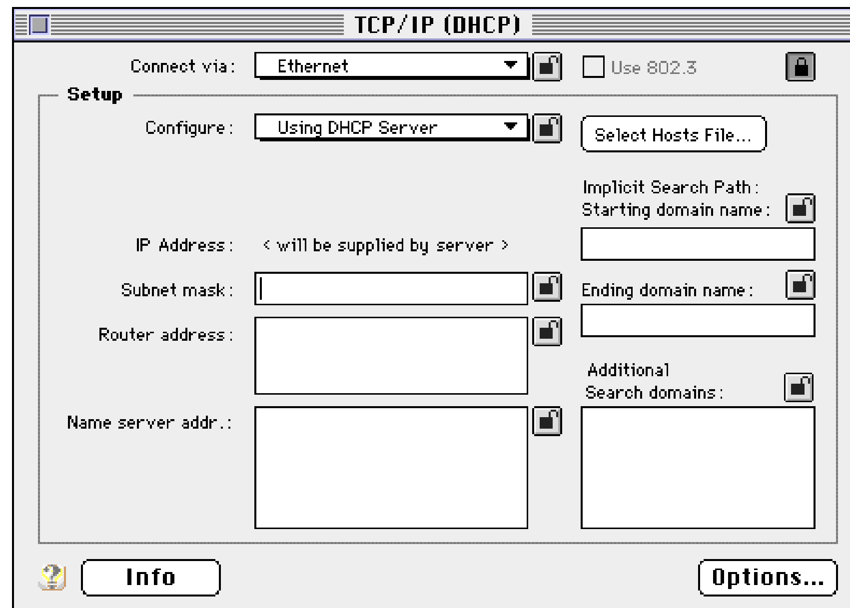
U bent nu verbonden met kennisnet.

4.4 Hoe maak ik met de Apple Macintosh een automatische verbinding met kennisnet?

Mac OS is het besturingssysteem van de Apple Macintosh. U kunt een netwerk van Apple computers aansluiten op kennisnet. Check eerst welke versie van Mac OS op uw Apple draait. Vanaf versie 7.5 kunt u met behulp van MacTCP en Open Transport gebruikmaken van DHCP om automatische IP-instellingen te verkrijgen, waarmee u een verbinding maakt met kennisnet. (Eventueel kunnen deze worden gevonden via de website van Apple: http://www.apple.com. Zoek daar naar ‘Open Transport’.)

Volg de volgende procedure om een automatische (dynamische) verbinding met kennisnet te maken:

- Open het regelpaneel ‘TCP/IP’.
- Maak indien nodig een nieuwe configuratie aan, bijvoorbeeld met de naam ‘kennisnet’, en keer terug naar het regelpaneel ‘TCP/IP’.



Figuur 26: Regelpaneel TCP/IP (DHCP)-configuratie

- Selecteer in het veld ‘Connect via’ de optie ‘Ethernet’.
- Selecteer vervolgens in het veld ‘Configure’ de optie ‘Using DHCP Server’ (via DHCP).

U hebt nu alle handelingen verricht om een automatische (dynamische) verbinding met kennisnet te maken. Alle overige instellingen worden door de server ingevuld.

- Bewaar deze configuratie en maak deze actief.

Let op!

Bij het herstarten van de computer of bij het ontwaken uit sluimerstand gooit Mac OS de verkregen gegevens weg en vervolgens ververst. Wanneer er geen verbinding met kennisnet is, zal na het verlopen van de geldigheidsduur de computer niet meer via TCP/IP kunnen werken. U zult dan opnieuw een verbinding met kennisnet moeten maken. De geldigheidsduur van de gegevens is echter vrij lang.

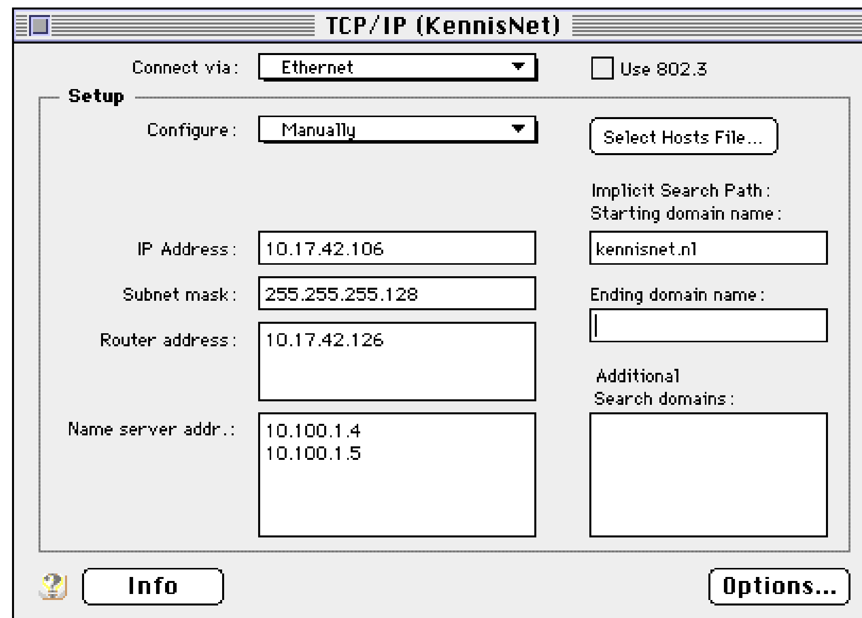
4.5 Hoe stel ik in Mac OS zelf de kennisnetinstellingen in?

Volg de volgende procedure om zelf een verbinding met kennisnet tot stand te brengen.

- Open het regelpaneel ‘TCP/IP’.
- Open de lijst met configuraties (command-K).

U kunt nu bestaande configuraties wijzigen of een nieuwe configuratie aanmaken. In dit voorbeeld gaan wij ervan uit dat u geen bestaande configuratie heeft.

- Maak een nieuwe configuratie aan, bijvoorbeeld met de naam ‘kennisnet’ en keer terug naar het regelpaneel ‘TCP/IP’.



Figuur 27: TCP/IP (kennisnet): statische IP-configuratie Mac OS

- Selecteer in het veld 'Connect via' de optie 'Ethernet'.
- Selecteer vervolgens in het veld 'Configure' de optie 'Manually'.
- Voer nu in het veld 'IP Address' het juiste IP-adres.
- Voer vervolgens in het veld 'Subnet mask' het juiste subnetmasker in.

Deze gegevens zou u van uw kabelmaatschappij ontvangen moeten hebben.

- Voer in het veld 'Router address' het IP-adres van de router in.

Wanneer u een reeks IP-adressen hebt ontvangen, dan is het IP-adres van de router normaal gesproken het hoogste of het laagste adres uit de aan u toegekende reeks. Eventueel kunt u het juiste adres opvragen via het Servicepunt Kennisnet.

- Voer in het veld 'Name server addr.' **altijd** de volgende IP-adressen in: '`212.178.5.4`' en '`212.178.5.5`'.
- Voer vervolgens in het veld 'Starting domain name' de domeinnaam '`kennisnet.nl`' in.
- Sluit het venster en bevestig de wijzigingen.

U bent nu verbonden met kennisnet.

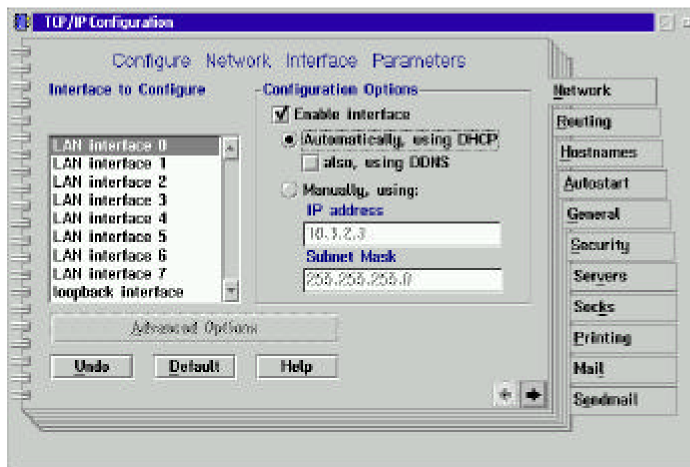
4.6 Hoe maak ik met OS/2 Warp een automatische (dynamische) verbinding met kennisnet?

U kunt met OS/2 Warp 3.0 of hoger (uit de blauwe doos, niet de rode), ook wel bekend als 'Warp Connect' (versie 3) en 'Merlin' (versie 4), gebruikmaken van TCP/IP om daarmee een verbinding met kennisnet te maken. Uiteraard dient u de ondersteuning voor TCP/IP geïnstalleerd te hebben. In het onderstaande voorbeeld is de UK-versie (Brits Engels) van OS/2 Warp 4 gebruikt.

Volg de volgende procedure om gebruik te maken van DHCP om een automatische (dynamische) verbinding met kennisnet te maken.

- Open het venster 'System Setup'.
- Selecteer 'TCP/IP Configuration (LAN)'.
- Selecteer het tabblad 'Network'.

Het volgende tabblad wordt geopend.



Figuur 28: OS/2 TCP/IP-configuratie via DHCP

- Selecteer uit de keuzelijst ‘Interface to Configure’ de eerste vrije LAN-interface. Wanneer u nog geen internet- of andere ethernetverbinding hebt, is dat ‘LAN interface 0’.
- Selecteer het aanvinkvakje ‘Enable Interface’.
- Selecteer vervolgens het keuzerondje ‘Automatically, using DHCP’.

U hebt nu alle handelingen verricht om een automatische (dynamische) verbinding met kennisnet te maken. Alle overige instellingen worden door de server ingevuld.

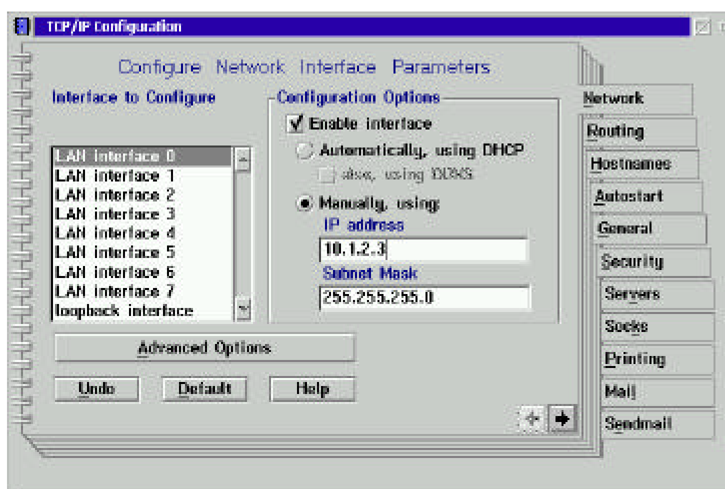
- Sluit het tabblad en bevestig dat u de wijzigingen wilt opslaan.
- Start uw computer opnieuw op om de nieuwe instellingen definitief te bewaren.

4.7 Hoe stel ik met OS/2 Warp zelf de kennisnetinstellingen in?

Volg de volgende procedure om zelf een verbinding met kennisnet tot stand te brengen.

- Open het venster ‘System Setup’.
- Selecteer ‘TCP/IP Configuration (LAN)’.
- Selecteer het tabblad ‘Network’.

Het volgende tabblad wordt geopend.



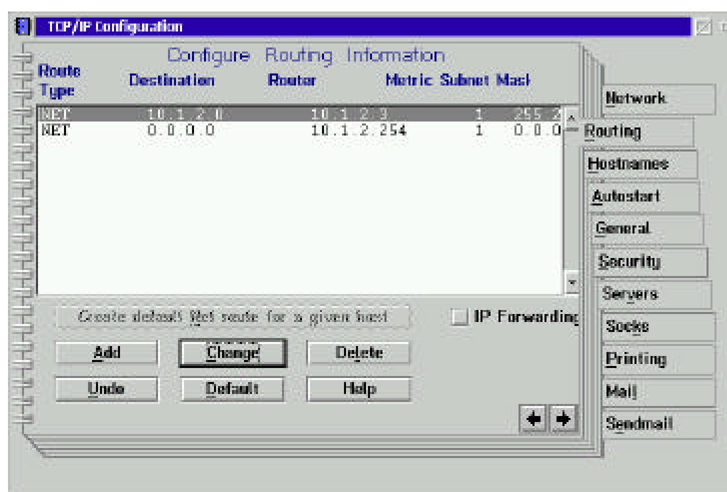
Figuur 29: OS/2 handmatige TCP/IP-configuratie

- Selecteer uit de keuzelijst ‘Interface to Configure’ de eerste vrije LAN-interface. Wanneer u nog geen internet- of andere ethernetverbinding hebt, is dat ‘LAN interface 0’.
- Selecteer het aanvinkvakje ‘Enable Interface’.
- Selecteer vervolgens het keuzerondje ‘Manually, using’.
- Voer nu in het veld ‘IP Adress’ het juiste IP-adres in.
- Voer vervolgens in het veld ‘Subnet Mask’ het juiste subnetmasker in.

Deze gegevens zou u van uw kabelmaatschappij ontvangen moeten hebben.

- Selecteer vervolgens het tabblad ‘Routing’.

Het onderstaande tabblad wordt geopend.



Figuur 30: TCP/IP Configuration, OS/2 IP-routes

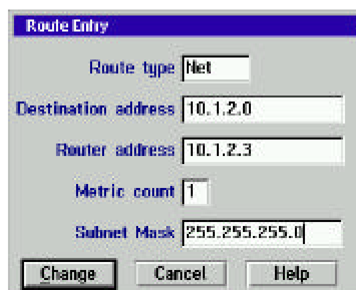
Op het tabblad ‘Routing’ kunt u routes instellen om het (netwerk)verkeer in goede banen te leiden. Normaliter stelt u op een werkstation slechts twee routes in:

1. de route naar het lokale netwerk;
2. de ‘default’-route, in dit geval de route naar kennisnet.

Allereerst stelt u de route naar het lokale netwerk in.

- Klik op de knop ‘Add’.

Het volgende venster wordt geopend.



Figuur 31: Route Entry: lokaal netwerk

- Voer in het veld ‘Destination address’ het IP-adres van uw lokale netwerk in.

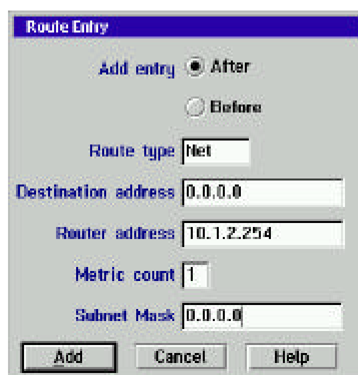
- Voer in het veld ‘Router address’ het IP-adres van de router in (in dit geval het IP-adres van *deze* machine).
- ‘Metric count’ is 1.
- Voer in het veld ‘Subnet Mask’ het subnetmasker in.
- Klik op ‘Change’ of ‘Add’ om de wijzigingen te bevestigen en terug te keren naar het tabblad ‘Routing’.

Nu kunt u de route naar kennisnet instellen.

- Klik weer op de knop ‘Add’.

Het volgende venster wordt geopend. In het venster ziet u twee keuzerondjes: ‘After’ en ‘Before’.

- Selecteer het keuzerondje ‘After’.



Figuur 32: Route Entry: default-route

- Voer in het veld ‘Destination address’ vier nullen in (‘0.0.0.0’).
- Voer in het veld ‘Router address’ het IP-adres van de router in.
- Metric count’ is 1.
- Voer in het veld ‘Subnet Mask’ als submasker weer vier nullen (‘0.0.0.0’).
- Klik op ‘Change’ of ‘Add’ om de wijzigingen te bevestigen en terug te keren naar het tabblad ‘Routing’.

Wanneer de OS/2-machine als router wordt gebruikt (bijvoorbeeld tussen uw lokale netwerk en kennisnet), kunt u eventueel op het tabblad ‘Routing’ de optie ‘IP Forwarding’ selecteren, zodat IP-verkeer door de machine kan worden afgehandeld. Hiervoor dienen echter ook meerdere ethernet-interfaces beschikbaar te zijn.

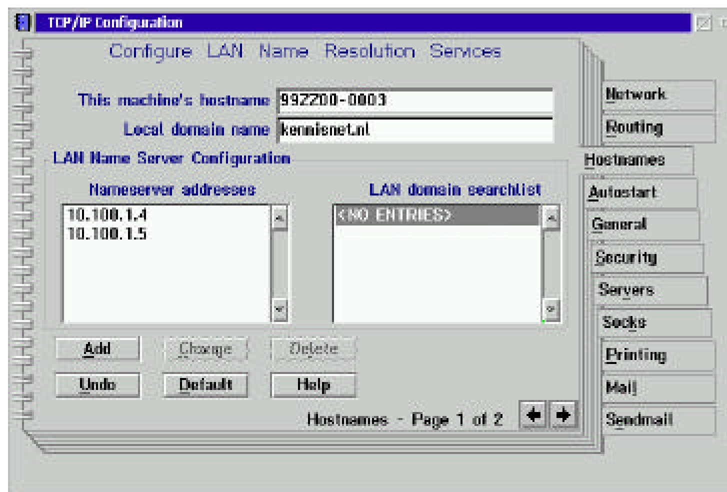


Figuur 33: OS/2 IP Forwarding

U hebt nu de routes naar het interne netwerk en kennisnet vastgelegd. Vervolgens kunt u de IP-adressen van de DNS-servers en de domeinnaam van kennisnet invoeren.

- Selecteer nu het tabblad ‘Hostnames’.

Het onderstaande tabblad wordt geopend.



Figuur 34: TCP/IP Configuration, OS/2 Hostname

- Voer in het veld ‘This machine’s hostname’ de naam van de machine in die u als router gebruikt.
- Voer in het veld ‘Local domain name’ de domeinnaam van kennisnet in: ‘kennisnet.nl’.

Vervolgens voert u de IP-adressen van de DNS-servers in.

- Klik op de keuzelijst ‘Nameserver addresses’ en klik vervolgens op de knop ‘Add’.
- Voer nu de volgende IP-adressen van de DNS-servers in: ‘212.178.5.4’ en ‘212.178.5.5’.

Het tabblad ‘Hostnames’ bestaat uit twee bladzijden. Op de tweede bladzijde van het tabblad kunt u eventueel namen van lokale machines of van machines waar veel contact mee is, opnemen in een lijst.

- Sluit het venster en bevestig dat u de wijzigingen wilt bewaren.
- Start de computer opnieuw op om de wijzigingen definitief op te slaan.

U hebt nu zelf de kennisnetinstellingen in OS2/Warp ingevoerd.

4.8 Hoe maak ik met BeOS een automatische (dynamische) verbinding met kennisnet?

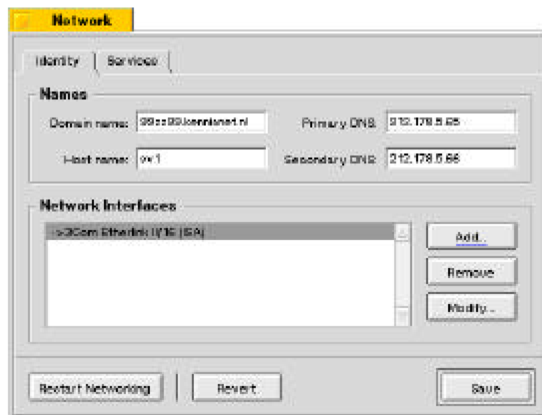
Ook met het besturingsysteem BeOS kan een automatische verbinding met kennisnet worden gemaakt. Belangrijk is om na te gaan of BeOS de hardware, zoals de in uw computer aanwezige netwerkkaart, ondersteunt. Raadpleeg hiervoor de website van Be, http://www.be.com/.

Volg de volgende procedure om een automatische verbinding met kennisnet tot stand te brengen.

- Open ‘Preferences’ en klik op het pictogram ‘Network’: 

.

Het scherm ‘Network’ wordt geopend. Dit scherm bevat twee tabbladen: ‘Identity’ en ‘Services’. Standaard wordt het tabblad ‘Identity’ geopend (u kunt het tabblad ‘Services’ negeren).



Figuur 35: Network, Identity: BeOS-netwerkinstellingen

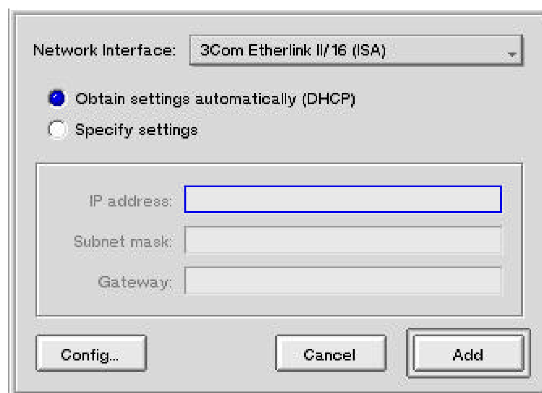
- Voer in het veld ‘Domain name’ de domeinnaam in van kennisnet.

Let op!

Uw domeinnaam is hier het BRIN-nummer van uw school inclusief het vestigingsnummer, gevolgd door ‘`.kennisnet.nl`’.

- Klik op de knop ‘Add’ (toevoegen) wanneer u nog geen netwerkinstellingen hebt vastgelegd.
- Klik op de knop ‘Modify’ (aanpassen) om uw bestaande netwerkinstellingen aan te passen.

Vervolgens wordt het volgende scherm geopend.



Figuur 36: Network Interface: BeOS DHCP

- Selecteer in de keuzelijst ‘Network Interface’ de juiste netwerkkaart.

Standaard is het keuzerondje ‘Obtain settings automatically (DHCP)’ geselecteerd, zodat het systeem automatisch een IP-adres krijgt toegewezen.

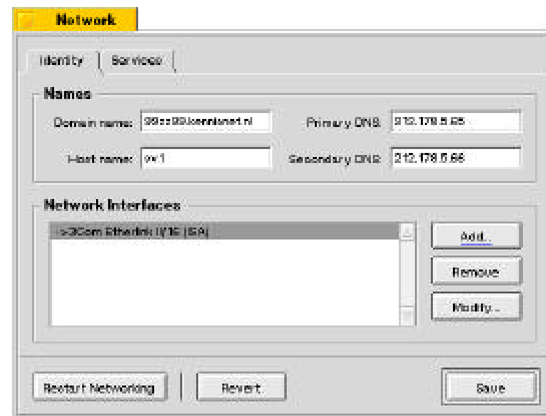
- Klik vervolgens op de knop ‘Add’ om de netwerkaansluiting toe te voegen of klik op ‘Modify’ om de aangepaste instellingen op te slaan en terug te keren naar het scherm ‘Network’.
- Klik vervolgens in het scherm ‘Network’ (Figuur 35) op de knop ‘Restart Networking’ om de nieuwe instellingen te activeren.
- Klik op de knop ‘Save’ om de nieuwe netwerkinstellingen te bewaren.

4.9 Hoe stel ik met BeOS zelf de kennisnetinstellingen in?

Volg de volgende procedure om zelf een verbinding met kennisnet tot stand te brengen.

- Open 'Preferences' en klik op het pictogram 'Network': .

Het scherm 'Network' wordt geopend. Dit scherm bevat twee tabbladen: 'Identity' en 'Services'. Standaard wordt het tabblad 'Identity' geopend.



Figuur 37: Network, Identity: BeOS-netwerkinstellingen

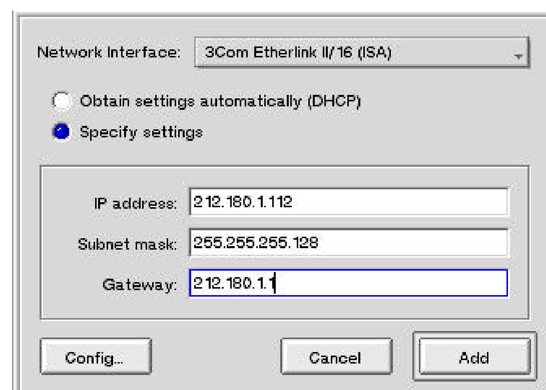
- Voer in het veld 'Domain name' de domeinnaam in van kennisnet

Let op!

Uw domeinnaam is hier het BRIN-nummer van uw school inclusief het vestigingsnummer, gevolgd door '`.kennisnet.nl`'.

- Voer in het veld 'Primary DNS' het IP-adres van de primaire DNS-server in: '`212.178.5.4`'.
- Voer in het veld 'Secondary DNS' het IP-adres van de secundaire DNS-server in: '`212.178.5.5`'.
- Klik op de knop 'Add' (toevoegen) wanneer u nog geen netwerkinstellingen hebt vastgelegd.
- Klik op de knop 'Modify' (aanpassen) om uw bestaande netwerkinstellingen aan te passen.

Het volgende scherm wordt geopend.



Figuur 38: Network Interface: BeOS statisch IP-adres

- Selecteer het keuzerondje 'Specify settings'.

De velden in het kader worden geactiveerd.

- Voer in het veld 'IP address' het IP-adres van de machine.
- Voer in het veld 'Subnet mask' het subnetmasker in
- Voer in het veld 'Gateway' het IP-adres van de router in.
- Klik op de knop 'Add' of de knop 'Modify' om de instellingen door te voeren.
- Klik vervolgens op de knop 'Restart Networking' om de instellingen te activeren.
- Klik op de knop 'Save' om de instellingen definitief op te slaan.

4.10 Hoe maak ik met Linux een verbinding met kennisnet?

Op deze vraag bestaat niet één antwoord. Onder de naam Linux gaan namelijk veel varianten schuil. Deze varianten zijn weliswaar op dezelfde programmeertaal gebaseerd, maar ogen anders. Ook de stappen om een verbinding met kennisnet te maken verschillen per variant van Linux. Dat is de reden waarom deze vraag hieronder alleen in de meest algemene zin kan worden beantwoord.

Raadpleeg de bijgeleverde softwaredocumentatie van Linux-versies zoals bijvoorbeeld Slackware, RedHat en Suse, hoe u een verbinding met een extern netwerk zoals kennisnet kunt maken.

4.10.1 Hoe maak ik met Linux een automatische (dynamische) verbinding met kennisnet?

Wanneer u een automatische verbinding met kennisnet wilt maken, dient uw Linux-versie voorzien te zijn van een zogenoemde DHCP-client. Bij de meeste versies van Linux wordt deze meegeleverd. Mocht deze ontbreken in uw versie van Linux, dan kunt u deze downloaden bij bijvoorbeeld: http://www.isc.org/products/DHCP/. Behalve het programma zelf vindt u hierin ook allerlei nuttige informatie over tot het DHCP-protocol.

Wanneer de DHCP-client is geïnstalleerd, zet u het commando om de DHCP-client op te starten in een opstartscript, zodat de client iedere keer wordt opgestart wanneer de machine opstart. Hoe u dit opstartscript moet invoeren, verschilt per versie van Linux. In de bijgeleverde documentatie van de DHCP-client vindt u enkele voorbeelden.

4.10.2 Hoe stel ik zelf de kennisnetinstellingen in Linux in?

Wanneer u zelf de instellingen (en dus IP-adressen) van kennisnet wilt invoeren, dient u behalve over een IP-adres en een subnetmasker ook over het IP-adres van de kennisnetrouter (het kennisnetmodem) en eventueel over de IP-adressen van de DNS-servers te beschikken.

Voor veel versies van Linux geldt dat u de netwerkkaart (ethernetkaart) handmatig van een IP-adres moet voorzien.

- Voer de opdracht regel '`Ifconfig eth0 212.180.0.3 netmask 255.255.255.0 up`' in.

In dit voorbeeld is het IP-adres '`212.180.0.3`'. Het subnetmasker is '`255.255.255.0`'. '`Eth0`' is het nummer van de eerste netwerkkaart die Linux tijdens het opstarten vindt. Deze gegevens kunt u ook in het opstartscript verwerken.

Behalve het IP-adres dient u ook de adressen van de DNS-servers in te voeren. In de directory '`/etc`' staat een bestand onder de naam '`resolv.conf`'.

- Open het bestand '`resolv.conf`' en voer de juiste gegevens in.

Het bestand kan er dan als volgt uitzien:

```
domain kennisnet.nl
search kennisnet.nl
nameserver 212.178.5.4
nameserver 212.178.5.5
```

Dit bestand is een zogenoemd configuratiebestand. Tijdens het opstarten van het netwerk raadpleegt Linux dit bestand. Dit bestand hoeft dus niet in een opstartscript te worden opgenomen.

Als laatste dient u op te geven dat al het verkeer naar kennisnet via de kennisnetrouter moet lopen.

- Voer de volgende opdrachtregels in:
  - `route add –net 212.180.0.0 netmask 255.255.255.0 eth0`’
  - `route add default gw 212.180.0.1 eth0`

In dit voorbeeld is ‘`212.180.0.1`’ het IP-adres van de kennisnetrouter.

Ook deze opdrachtregels kunt u in het opstartscript zetten.

Wanneer u met een versie van Linux werkt die beschikt over een grafische interface, dan hoeft u de meeste van bovenstaande instellingen niet handmatig in te voeren. Wel moeten altijd de IP-adressen van het werkstation (pc), de DNS-servers en de kennisnetrouter worden ingevoerd.

Meer informatie over het handmatig configureren van het netwerk met een Linux-machine kunt u vinden op de website: http://www.linuxdoc.org/HOWTO/Net-HOWTO/index.html.

4.11 Hoe maak ik met Windows 3.1x een automatische (dynamische) verbinding met kennisnet?

Windows 3.1x is een van de eerste versies van Windows en stamt nog uit de tijd dat internet nog niet was uitgegroeid tot het medium dat het nu is. Standaard kunt u met Windows 3.1x geen automatische verbinding met kennisnet maken. Een automatische verbinding maakt gebruik van het DHCP-protocol en dat wordt door Windows 3.1x niet ondersteund.

Wanneer u niettemin met Windows 3.1x een automatische verbinding met kennisnet wilt maken, dan kunt u het volgende doen:

- Windows 3.11 (Windows for Workgroups) kan geschikt worden gemaakt voor kennisnet (dus voor de protocollen TCP/IP en DHCP). Op de FTP-site van Microsoft is een patch beschikbaar waarmee u Windows 3.1x geschikt kunt maken voor kennisnet: ftp://ftp.microsoft.com/bussys/clients/wfw/. Selecteer het programma met de naam ‘tcp32b.exe’. Hieronder wordt uitgelegd hoe u ‘tcp32b.exe’ kunt installeren.

Let op!

*Selecteer **niet** de patch met de naam TCPWFW.*

- U kunt aan al uw werkstations handmatig IP-adressen toekennen.
- U kunt een zogenoemde BOOTP-server opzetten en DHCP (waarmee u een automatische verbinding met kennisnet maakt) voor uw IP-reeks laten uitschakelen. Zie deel V voor meer informatie. De DHCP-server van ‘The Internet Software Consortium’ (ISC) biedt ook BOOTP-functionaliteit. Raadpleeg de website van ISC voor meer informatie: http://www.isc.org/.
- Mocht u bovenstaande mogelijkheden te bewerkelijk vinden, dan kunt u als laatste optie uw systemen opwaarderen naar Windows 95/98/NT of Win-OS/2 (OS/2 Warp 3 of 4, ‘blue box’). Zo kunt u alsnog gebruikmaken van DHCP en automatisch een verbinding met kennisnet maken.

Let op!

Ga na of de door u in gebruik zijnde hardware (pc’s) een overstap naar een nieuw besturingssysteem toelaat!

Raadpleeg het Servicepunt Kennisnet indien u zelf een BOOTP-server wilt opzetten of indien u nog aanvullende vragen hebt.

4.11.1 Hoe maak ik Windows 3.1x geschikt voor kennisnet: installatie van TCP32B

In het onderstaande voorbeeld is de Engelse versie van Windows 3.1x gebruikt.Vergelijk de schermen eventueel met uw Nederlandse versie.

- Ga naar de volgende FTP-site van Microsoft (ftp://ftp.microsoft.com/bussys/clients/wfw/) en download de patch met de naam ‘tcp32b.exe’.
- Bewaar het bestand ‘tcp32b.exe’ in een map waar u uw tijdelijke bestanden bewaart of maak een nieuwe map (bijvoorbeeld: `c:\temp`).
- Pak het bestand ‘tcp32b.exe’ uit door erop te dubbelklikken.

Het programma ‘tcp32b.exe’ wordt in dezelfde map uitgepakt als het eerder is bewaard.

- Klik vanaf het bureaublad op het pictogram ‘Hoofdgroep’ (‘Main’).

Het venster ‘Hoofdgroep’ (‘Main’) wordt geopend.



Figuur 39: Hoofdgroep (Main)

- Klik op het pictogram ‘Windows Setup’.

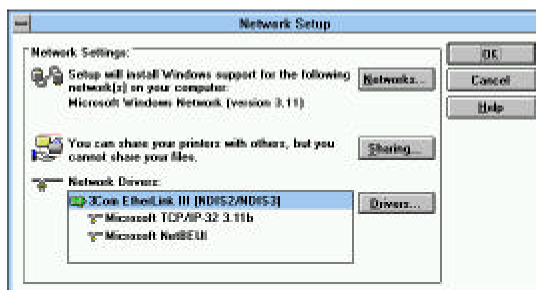
Het venster ‘Windows Setup’ wordt geopend.



Figuur 40: Windows Setup

- Kies uit menu ‘Opties’ (‘Options’) de optie ‘Netwerkconfiguratie’ (‘Change Network Settings...’).

Het venster ‘Network Setup’ wordt geopend.

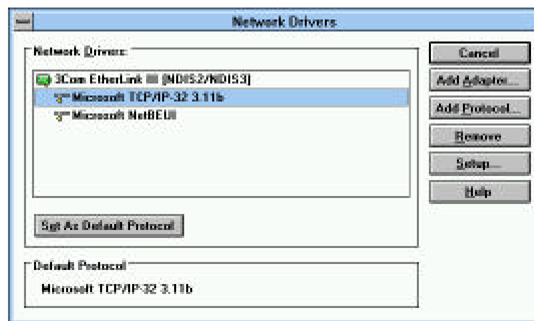


Figuur 41: Netwerkconfiguratie (Network Setup)

In het venster ‘Netwerkconfiguratie’ kunt u verschillende soorten netwerken installeren.

- Selecteer uw netwerkkaart (in bovenstaand voorbeeld is dat 3COM Etherlink III [INDIS2/INDIS3]) en klik op de knop ‘Stuurprogramma’s…’ (‘Drivers...’).

Het venster ‘Network Drivers’ wordt geopend.



Figuur 42: Stuurprogramma's (Network Drivers)

Verwijder eerst de bestaande stuurprogramma's voor TCP/IP.

- Selecteer het bestaande stuurprogramma's voor TCP/IP en klik op de knop 'Verwijderen' ('Remove').
- Bevestig uw keuze.

Let op!

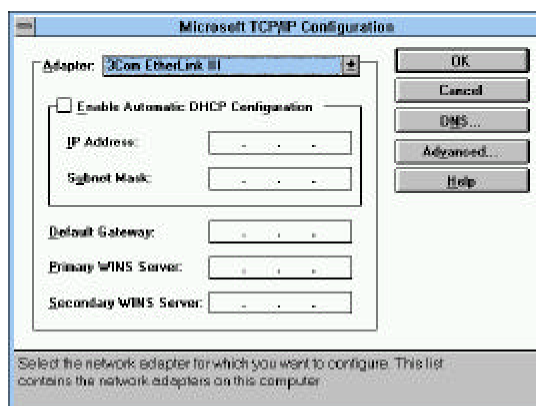
Laat andere netwerkprotocollen intact!

- Klik vervolgens op de knop 'Protocol toevoegen' ('Add Protocol...').
- Selecteer uit de keuzelijst de optie 'Unlisted or updated protocol' en klik op de knop 'OK'.

Vervolgens kunt u uit het *uitgepakte* bestand 'tcp32b.exe', dat u eerder in een map heeft bewaard, het juiste TCP/IP-protocol selecteren.

- Klik daartoe op de knop 'Bladeren' ('Browse') en selecteer de map waar u het *uitgepakte* bestand 'tcp32b.exe' hebt bewaard, en klik op de knop 'OK'
- Selecteer het protocol 'Microsoft TCP/IP-32 for Windows for Workgroups 3.11' en klik op de knop 'OK'.

De installatie van het TCP/IP-protocol wordt gestart. Na de installatie verschijnt het scherm 'Microsoft TCP/IP Configuration'.



Figuur 43: Microsoft TCP/IP-configuratie

- Selecteer het aanvinkvakje 'Enable Automatic DHCP Configuration' en klik op de knop 'OK'.
- Start uw computer opnieuw op om de verbinding te activeren.

U hebt nu alle handelingen verricht om een automatische verbinding met kennisnet te maken.

5. Software-instellingen voor e-mail, webbrowsers en andere applicaties

Nadat u een verbinding met kennisnet hebt gemaakt, is het tijd voor de volgende stap: het invoeren van de instellingen voor e-mailprogramma's (bijvoorbeeld: Microsoft Outlook Express of Netscape Communicator), webbrowsers (bijvoorbeeld: Microsoft Internet Explorer of Netscape Communicator) en andere applicaties (bijvoorbeeld: FTP- en Telnet-programma's).

Met deze programma's kunt u daadwerkelijk 'kennisnet op'. Zo kunt u met programma's als Outlook Express e-mail versturen en ontvangen en kunt u met Internet Explorer en Netscape Communicator websites bekijken. Met FTP-programma's kunt u bestanden up- en downloaden.

5.1 Hoe kan ik met Netscape Communicator kennisnet op?

Met Netscape Communicator kan worden 'gesurft' op kennisnet, bijvoorbeeld naar web- en naar FTP-sites. Ook e-mail en nieuws (nieuws- of discussiegroepen) kunnen worden gelezen. Deze toepassingen zullen stuk voor stuk aan bod komen.

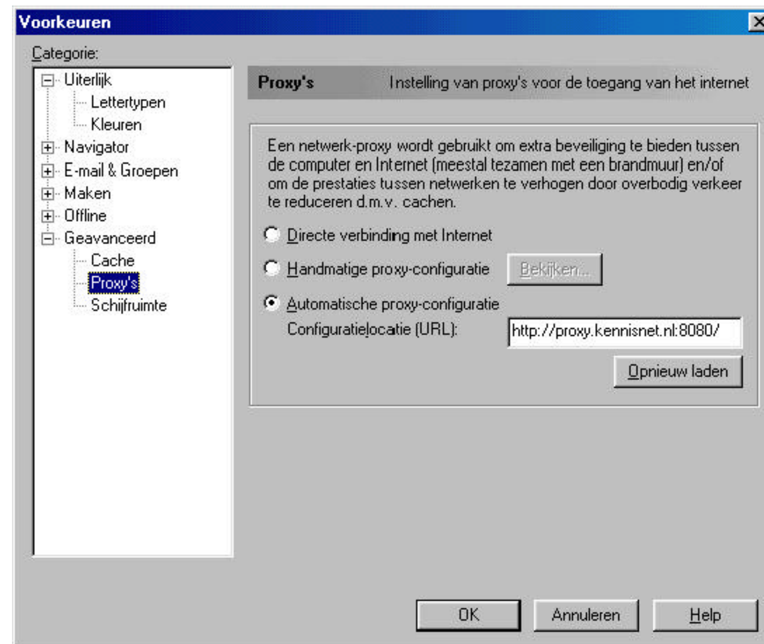
5.1.1 Netscape Communicator: instellingen voor kennisnet

Om te kunnen surfen op kennisnet (en het internet), moet de zogenoemde 'proxy'-configuratie worden ingesteld. De proxy is in grote lijnen een machine die het netwerkverkeer controleert en beveiligt tegen indringers van buitenaf. Via de proxy kunt u naar buiten, maar kunnen anderen niet naar binnen.

De instellingen voor de proxy worden automatisch door proxy-machines van kennisnet aangeleverd. U hoeft in Netscape Communicator alleen het 'adres' in te voeren waar Netscape de instellingen moet 'ophalen'.

Volg de volgende procedure om de proxy -instellingen in te voeren.

- Open Netscape Communicator.
- Kies uit het menu 'Bewerken' de optie'Voorkeuren'.
- Klik in de keuzelijst 'Categorie' op de optie 'Geavanceerd' en selecteer vervolgens de optie 'Proxy's'.



Figuur 44: Voorkeuren, Geavanceerd, Proxy's

- Selecteer het keuzerondje 'Automatische proxy-configuratie'.
- Voer in het veld 'Configuratielocatie (URL)' het adres van de server in: '`http://proxy.kennisnet.nl:8080`'.
- Klik op de knop 'OK'.

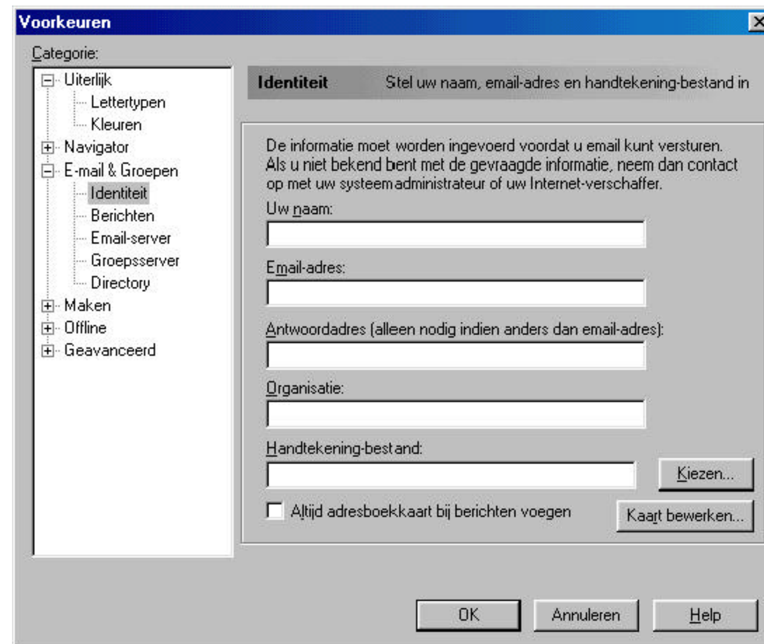
U kunt nu met Netscape Communicator 'surfen' op kennisnet.

5.1.2 Wie is wie op kennisnet: uw identiteit instellen in Netscape Communicator

Wanneer u e-mail verstuurt moet de ontvanger kunnen zien van wie de e-mail afkomstig is. Dat is de reden waarom u uw identiteit (personalia) kunt invoeren in Netscape Communicator.

Volg de volgende procedure om uw identiteit in te voeren.

- Open Netscape Communicator.
- Kies uit het menu 'Bewerken' de optie 'Voorkeuren'.
- Klik in de keuzelijst 'Categorie' op de optie 'E-mail & Groepen' en selecteer de optie 'Identiteit'.



Figuur 45: Voorkeuren, E-mail & Groepen, Identiteit

- Voer in het veld 'Uw naam' uw naam in.
- Voer in het veld 'E-mail -adres' uw e-mailadres in (dit is de gebruikersnaam met daarachter '@kennisnet.nl').

Het veld 'Antwoordadres' hoeft u niet in te vullen.

- Voer in het veld 'Organisatie' de naam van uw school in.

Het veld 'Handtekening-bestand' kunt u overslaan.

- Klik op de knop 'OK' om de instellingen te bewaren.

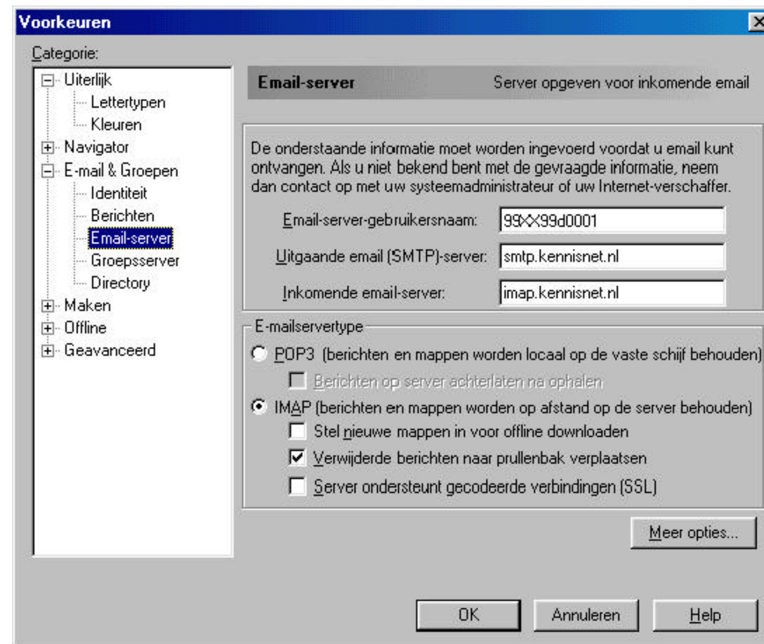
U hebt nu uw identiteit in Netscape Communicator ingevoerd.

5.1.3 Netscape Communicator: instellingen voor e-mail

U kunt met Netscape Communicator niet alleen surfen op kennisnet, u kunt met Netscape ook e-mail verzenden en ontvangen. Om dat te kunnen doen, moet Netscape bijvoorbeeld weten waar e-mail moet worden opgehaald.

Volg de volgende procedure om uw e-mailinstellingen in te voeren.

- Open Netscape Communicator.
- Kies uit het menu 'Bewerken' de optie 'Voorkeuren'.
- Klik in de keuzelijst 'Categorie' op de optie 'E-mail & Groepen' en selecteer de optie 'E-mail-server'.



Figuur 46: Voorkeuren, E-mail & Groepen, E-mailserver

- Voer in het veld ‘E-mail-server-gebruikersnaam’ uw gebruikersnaam voor kennisnet in.
- Voer in het veld ‘Uitgaande e-mail (SMTP)-server’ het adres van de server in: ‘`smtp.kennisnet.nl`’.

Voor binnenkomende e-mail kunt u vervolgens kiezen tussen twee verschillende manieren (protocollen) om een e-mail te ontvangen (POP3 of IMAP). Raadpleeg deel VI om te bepalen welk protocol in uw geval geschikt is.

- Voer in het veld ‘Inkomende e-mail-server’ ‘`pop.kennisnet.nl`’ als u voor het POP3-protocol hebt gekozen.
- Voer in het veld ‘Inkomende e-mail-server’ ‘`imap.kennisnet.nl`’ als u voor het IMAP-protocol hebt gekozen.
- Klik op de knop ‘OK’ om de instellingen te bewaren.

U kunt nu e-mail versturen en ontvangen met Netscape Communicator.

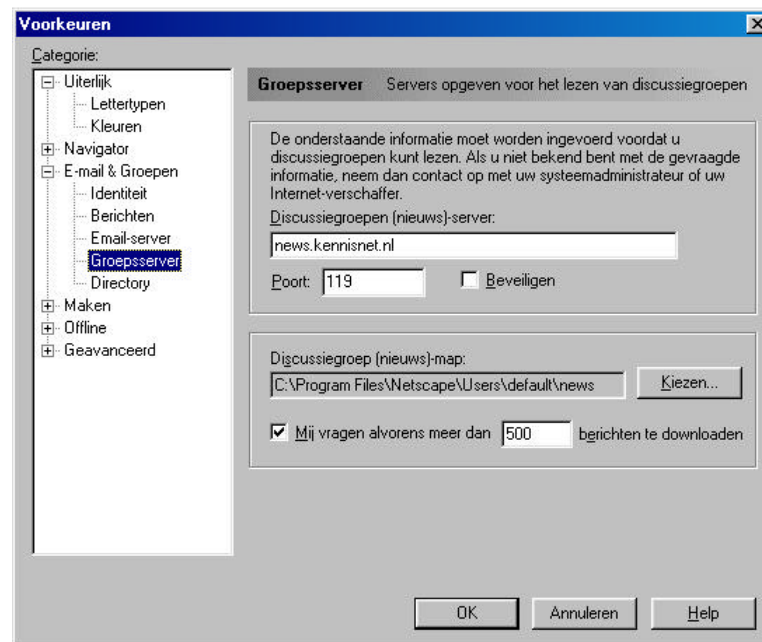
5.1.4 Netscape Communicator: instellingen voor nieuwsgroepen

U kunt met gelijkgestemden een nieuwsgroep opzetten om informatie over bepaalde onderwerpen uit te wisselen. U kunt ook bestaande nieuwsgroepen bezoeken. Zo kunt u berichten versturen naar een nieuwsgroep of berichten of bestanden downloaden uit een nieuwsgroep.

Om met Netscape Communicator van nieuwsgroepen gebruik te kunnen maken, moet Netscape weten waar de nieuwsgroepen zich bevinden.

Volg de volgende procedure om uw instellingen voor nieuwsgroepen in te voeren.

- Open Netscape Communicator.
- Kies uit het menu ‘Bewerken’ de optie ‘Voorkeuren’.
- Klik in de keuzelijst ‘Categorie’ op de optie ‘E-mail & Groepen’ en selecteer de optie ‘Groepsserver’.



Figuur 47: Voorkeuren, E-mail & Groepen, Groepsserver

- Voer in het veld ‘Discussiegroepen (nieuws)-server’ de naam van de nieuwsserver in :‘`news.kennisnet.nl`’.
- Voer in het veld ‘Poort’ het standaardpoortnummer in: 119.

De overige instellingen kunt u ongemoeid laten.

- Klik op de knop ‘OK’ om de instellingen op te slaan.

U kunt nu nieuwsgroepen bezoeken op kennisnet.

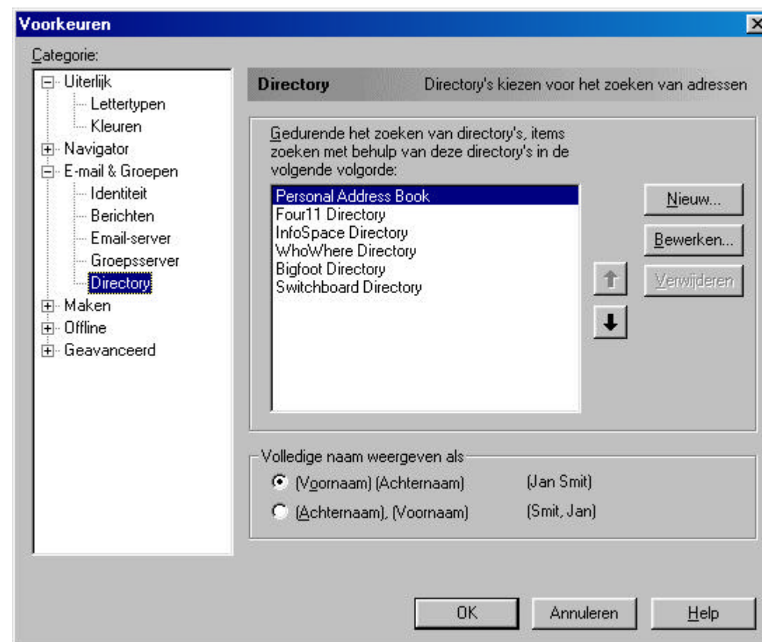
5.1.5 Zoeken naar personen: adreslijst op kennisnet (LDAP)

Om op kennisnet personen te kunnen opzoeken, is een publiek toegankelijke adreslijst opengesteld. Dit noemen we een zogenoemde LDAP-server. Deze machine bevat de e-mailadressen van alle kennisnetgebruikers.

Om met Netscape Communicator gebruik te maken van deze adreslijst, moet u het adres van de LDAP-server in Netscape invoeren.

Volg de volgende procedure om uw instellingen voor LDAP in Netscape in te voeren.

- Open Netscape Communicator.
- Kies uit het menu ‘Bewerken’ de optie ‘Voorkeuren’.
- Klik in de keuzelijst ‘Categorie’ op de optie ‘E-mail & Groepen’ en selecteer de optie ‘Directory’.



Figuur 48: Voorkeuren, E-mail & Groepen, Directory

- Klik op de knop ‘Nieuw...’ om kennisnet aan de lijst met zoekdirectory’s toe te voegen.[6]

Het venster ‘Directory-server-eigenschap’ wordt geopend.



Figuur 49: Directory server eigenschap

- Voer in het veld ‘Beschrijving’ een willekeurige, maar herkenbare naam in, bijvoorbeeld ‘kennisnet’.
- Voer in het veld ‘LDAP-server’ het adres van de LDAP-server in: ‘`ldap.kennisnet.nl`’.

In het veld ‘Zoekwortel’ kunt u een aantal zoekopties (restricties) invoeren. Deze zoekopties leggen beperkingen op aan wat, waar wordt gezocht.

- Voer in het veld ‘Zoekwortel’ de volgende restrictie in: ‘`c=nl o=kennisnet`’.

U hebt hiermee ingevoerd dat u alleen in Nederland wilt zoeken. De overige instellingen kunt u ongemoeid laten.

- Klik op de knop ‘OK’ om de instellingen op te slaan.

U kunt nu met behulp van Netscape Communicator de adreslijst op kennisnet raadplegen.

[6] Zeer waarschijnlijk zijn door de firewall-restricties de andere genoemde LDAP-servers niet bereikbaar vanaf kennisnet.

5.2 Hoe kan ik met Microsoft Internet Explorer kennisnet op?

Met Microsoft Internet Explorer kan alleen worden gesurft op kennisnet, bijvoorbeeld naar web- of naar FTP-sites. Om e-mail of nieuws (nieuwsgroepen) te kunnen lezen, heeft u Microsoft Outlook (Express) nodig.

Zoals van de meeste computerprogramma's zijn ook van de Internet Explorer verschillende versies in de omloop. Omdat Microsoft Internet Explorer 4 en Microsoft Internet Explorer 5 sterk van elkaar verschillen maar beide versies veel worden gebruikt, wordt het invoeren van de kennisnetinstellingen voor beide versies hieronder behandeld.

5.2.1 Microsoft Internet Explorer 4: instellingen voor kennisnet

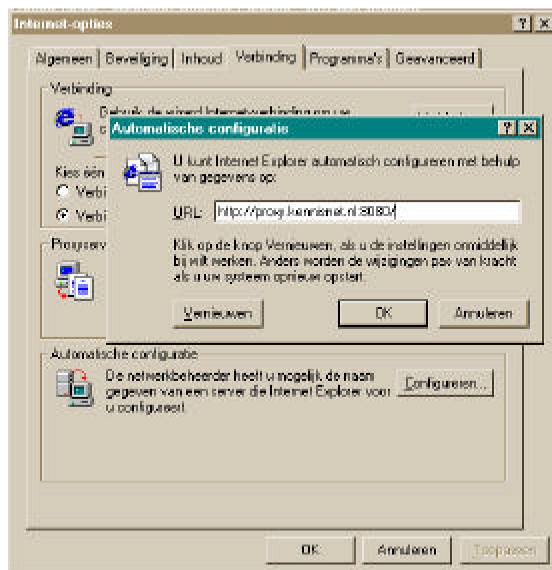
Om te kunnen surfen op kennisnet (en het internet), moet de zogenoemde 'proxy'-configuratie worden ingesteld. De proxy is in grote lijnen een machine die het netwerkverkeer controleert en beveiligt tegen indringers van buitenaf. Via de proxy kunt u naar buiten, maar kunnen anderen niet naar binnen.

De instellingen voor de proxy worden automatisch door proxy-machines van kennisnet aangeleverd. U hoeft in Microsoft Internet Explorer 4 alleen het 'adres' in te voeren waar de Internet Explorer de instellingen moet 'ophalen'.

Volg de volgende procedure om de proxy-instellingen in te voeren.

- Open Microsoft Internet Explorer 4.
- Kies uit het menu 'Beeld' de optie 'internet-opties'.
- Klik op het tabblad 'Verbinding'.
- Klik vervolgens onder 'Automatische configuratie' op de knop 'Configureren'.

Het venster 'Automatische configuratie' wordt geopend.



Figuur 50: Internet-opties, Verbinding, Automatische configuratie

- Voer in veld 'URL' het adres van de proxy-server in: '`http://proxy.kennisnet.nl:8080`'.
- Klik op de knop 'OK' om de instellingen op te slaan en terug te keren naar het scherm 'internet-opties'.
- Klik in het venster 'internet-opties' op de knop 'OK' om het venster te sluiten.

U kunt nu met Microsoft Internet Explorer 4 surfen op kennisnet en internet.

5.2.2 Microsoft Internet Explorer 5: instellingen voor kennisnet

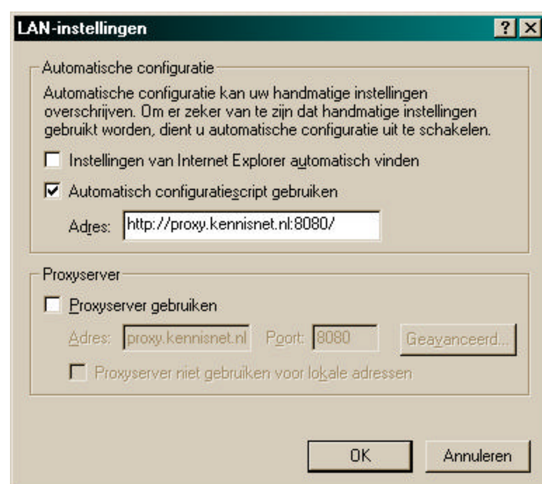
Om te kunnen surfen op kennisnet (en het internet), moet de zogenoemde proxy-configuratie worden ingesteld. De proxy is in grote lijnen een machine die het netwerkverkeer controleert en beveiligt tegen indringers van buitenaf. Via de proxy kunt u naar buiten, maar kunnen anderen niet naar binnen.

De instellingen voor de proxy worden automatisch door proxy-machines van kennisnet aangeleverd. U hoeft in Microsoft Internet Explorer 5 alleen het ‘adres’ in te voeren waar de Internet Explorer de instellingen moet ‘ophalen’.

Volg de volgende procedure om de proxy -instellingen in te voeren.

- Open Microsoft Internet Explorer 5.
- Kies uit het menu ‘Beeld’ de optie ‘internet-opties’.
- Klik op het tabblad ‘Verbinding’.
- Klik vervolgens op de knop ‘Lan-instellingen’.

Het venster ‘LAN-instellingen’ wordt geopend.



Figuur 51: internet-opties, LAN-instellingen

- Selecteer het aanvinkvakje ‘Automatisch configuratiescript gebruiken’.
- Voer in veld ‘Adres’ het adres van de proxy -server in: `http://proxy.kennisnet.nl:8080`.
- Klik op de knop ‘OK’ om de instellingen op te slaan en terug te keren naar het scherm ‘internet-opties’.
- Klik in het venster ‘internet-opties’ op de knop ‘OK’ om het venster te sluiten.

U kunt nu met Microsoft Internet Explorer 5 surfen op kennisnet en internet.

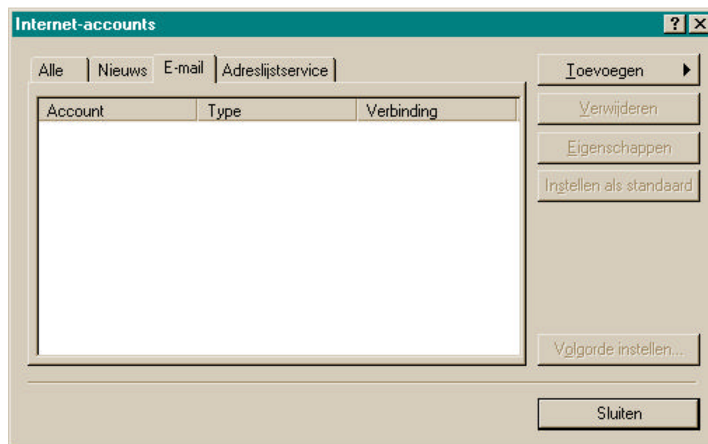
5.3 Instellingen voor e-mail: Microsoft Outlook of Outlook Express

U kunt met Microsoft Outlook of Outlook Express e-mail verzenden en ontvangen. Om dat te kunnen doen, moet Microsoft Outlook (Express) bijvoorbeeld weten waar e-mail moet worden opgehaald.

Volg de volgende procedure om uw e-mailinstellingen in te voeren.

- Open Outlook of Outlook Express.
- Kies uit het menu ‘Beeld’ de optie ‘internet-opties’.

Het venster ‘internet-accounts’ wordt geopend. Dit venster heeft drie (Outlook) of vier (Outlook Express) tabbladen.

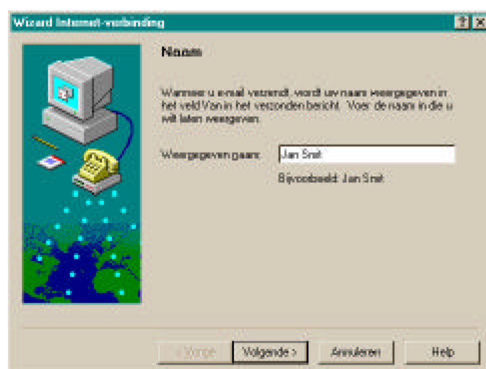


Figuur 52: internet-accounts in Outlook (Express), E-mail

- Selecteer het tabblad ‘E-mail’.
- Klik op de knop ‘Toevoegen’ en selecteer ‘E-mail...’

Vervolgens wordt u in een aantal stappen door een Wizard geleid om een nieuwe e-mailaccount aan te maken.

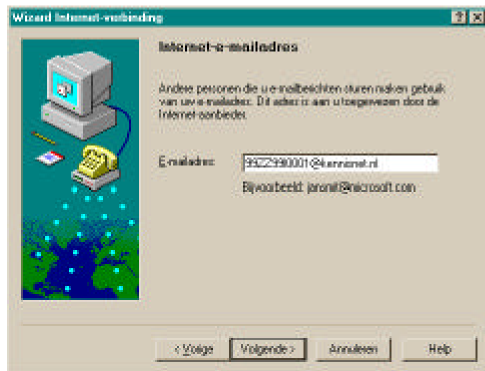
Nadat u ‘E-mail...’ hebt geselecteerd verschijnt het eerste scherm van de ‘Wizard internet-verbindingen’.



Figuur 53: Wizard internet-verbinding, Naam

Stap 1: voor- en achternaam invoeren

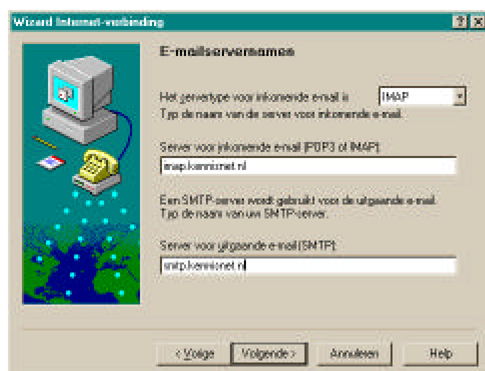
- Voer in het veld ‘Weergegeven naam’ uw voor- en achternaam in.
- Klik op de knop ‘Volgende>’.



Figuur 54: Wizard internet-verbinding, internet-e-mailadres

Stap 2: e-mailadres invoeren

- Voer in het veld 'E-mailadres' uw e-mailadres in (*gebruikersnaam*@kennisnet.nl).
- Klik op de knop 'Volgende>'.

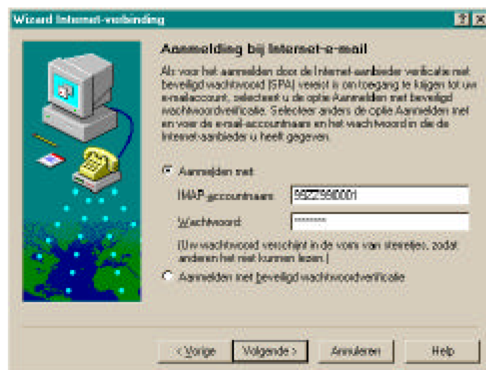


Figuur 55: Wizard internet-verbinding, E-mailservernamen

Stap 3: servernamen invoeren

Voor binnenkomende e-mail kunt u kiezen tussen twee verschillende manieren (protocollen) om een e-mail te ontvangen (POP3 of IMAP). Raadpleeg deel VI om te bepalen welk protocol in uw geval geschikt is.

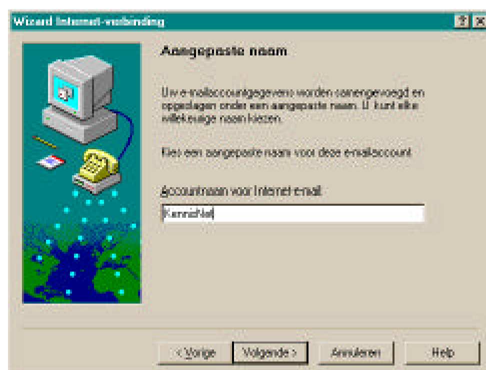
- Voer in het veld 'Server voor inkomende e-mail (POP3 of IMAP)' '`pop.kennisnet.nl`' als u voor het POP3-protocol hebt gekozen.
- Voer in het veld 'Inkomende e-mail-server' '`imap.kennisnet.nl`' als u voor het IMAP-protocol hebt gekozen.
- Voer in het veld 'Server voor uitgaande e-mail (SMTP)' het adres van de server in: '`smtp.kennisnet.nl`'.
- Klik op de knop 'Volgende>'.



Figuur 56: Wizard internet-verbinding, Aanmelding

Stap 4: aanmelden

- Selecteer het keuzerondje ‘Aanmelden met’.
- Voer in het veld ‘IMAP-accountnaam’ uw gebruikersnaam in wanneer u voor IMAP hebt gekozen (*gebruikersnaam*@kennisnet.nl).
- Voer in het veld ‘Wachtwoord’ uw wachtwoord in.
- Klik op de knop ‘Volgende>’.



Figuur 57: Wizard internet-verbinding, Aangepaste naam

Stap 5: omschrijving account

- Voer in het veld ‘Accountnaam voor internet-e-mail’ een naam naar keuze in (bijvoorbeeld: KennisNet).
- Klik op de knop ‘Volgende>’.



Figuur 58: Wizard internet-verbinding, Type verbinding

Stap 6: type verbinding kiezen

- Selecteer het keuzerondje ‘LAN-netwerk gebruiken’.
- Klik op de knop ‘Volgende>’.



Figuur 59: Wizard internet-verbinding, Voltooien

Stap 7: Voltooien

- Klik op de knop ‘Voltooien’ om de instellingen op te slaan.

U beschikt nu over een e-mailaccount.

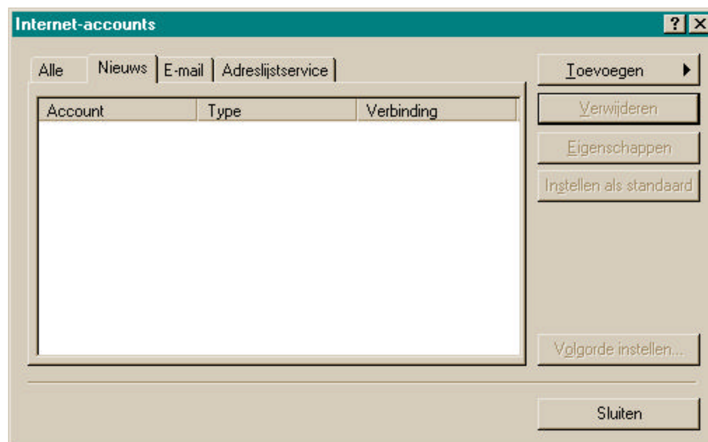
5.3.1 Microsoft Outlook Express: instellingen voor nieuwsgroepen

U kunt alleen met Outlook Express nieuwsgroepen bezoeken (Outlook biedt deze optie niet). Om dat te kunnen doen, moet Microsoft Outlook Express weten waar de nieuwsgroepen zich bevinden.

Volg de volgende procedure om uw instellingen voor nieuwsgroepen in te voeren.

- Open Outlook of Outlook Express.
- Kies uit het menu ‘Extra’ de optie ‘Accounts’.

Het venster ‘internet-accounts’ wordt geopend.



Figuur 60: internet-accounts, Nieuws

- Selecteer het tabblad ‘Nieuws’.
- Klik op ‘Toevoegen’ en selecteer ‘Nieuws…’.

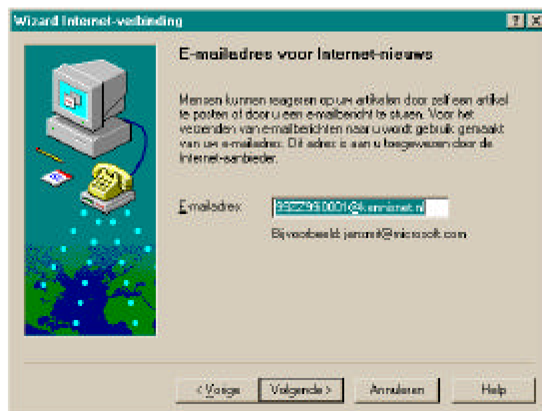
Vervolgens wordt u in een aantal stappen door een Wizard geleid om een nieuwsserver toe te voegen. Nadat u ‘Nieuws...’ hebt geselecteerd, verschijnt het eerste scherm van de ‘Wizard internet-verbindingen’.



Figuur 61: Wizard internet-verbinding, Naam

Stap 1: voor- en achternaam invoeren

- Voer in het veld ‘Weergegeven naam’ uw voor- en achternaam in.
- Klik op de knop ‘Volgende>’.



Figuur 62: Wizard internet-verbinding, E-mailadres voor internet-nieuws

Stap 2: e-mailadres invoeren

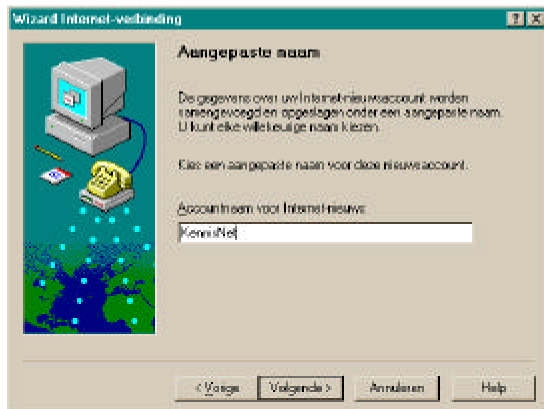
- Voer in het veld ‘E-mailadres’ uw e-mailadres in (*gebruikersnaam*@kennisnet.nl).
- Klik op de knop ‘Volgende>’.



Figuur 63: Wizard internet-verbinding, Naam van internet-nieuwsserver

Stap 3: servernaam invoeren

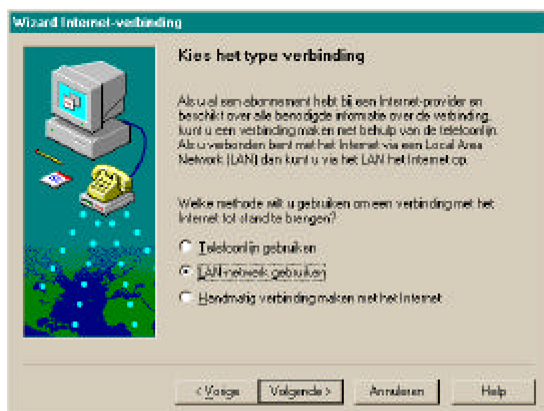
- Voer in het veld ‘Nieuwsserver (NNTP)’ het adres van server in: `news.kennisnet.nl`’ server.
- Klik op de knop ‘Volgende>’.



Figuur 64: Wizard internet-verbinding, Aangepaste naam

Stap 5: omschrijving account

- Voer in het veld ‘Accountnaam voor internet-e-mail’ een naam naar keuze in (bijvoorbeeld: KennisNet).
- Klik op de knop ‘Volgende>’.



Figuur 65: Wizard internet-verbinding, Type verbinding

Stap 6: type verbinding kiezen

- Selecteer het keuzerondje ‘LAN-netwerk gebruiken’.
- Klik op de knop ‘Volgende>’.



Figuur 66: Wizard internet-verbinding, Voltooien

Stap 7: Voltooien

- Klik op de knop 'Voltooien' om de instellingen op te slaan.

U beschikt nu over een nieuwsaccount.

5.3.2 Zoeken naar personen: adreslijst op kennisnet (LDAP)

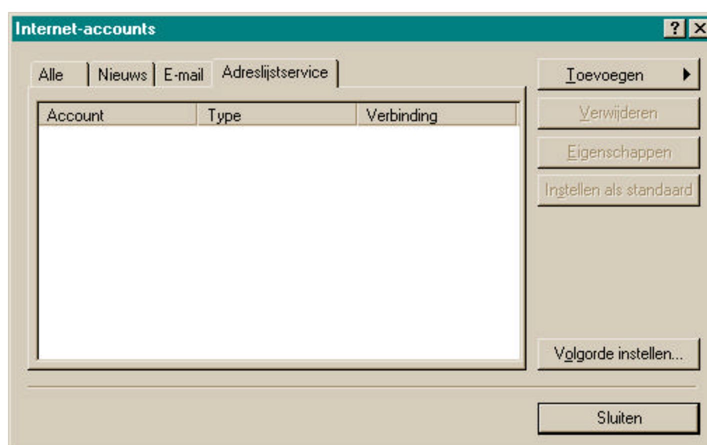
Om op kennisnet personen te kunnen opzoeken, is een publiek toegankelijke adreslijst opengesteld. Dit noemen we een zogenoemde LDAP-server. Deze machine bevat de e-mailadressen van alle kennisnetgebruikers.

Om met Microsoft Outlook gebruik te maken van deze adreslijst, moet u het adres van de LDAP-server in Outlook invoeren.

Volg de volgende procedure om uw instellingen voor de adreslijstservice in te voeren.

- Open Outlook of Outlook Express.
- Kies uit het menu 'Extra' de optie 'Accounts'.

Het venster 'internet-accounts' wordt geopend.



Figuur 67: internet-accounts, Adreslijstservice

- Selecteer het tabblad 'Adreslijstservice' en klik op de knop 'Toevoegen'.

Vervolgens wordt u in een aantal stappen door een Wizard geleid om een adreslijst toe te voegen.

Nadat u 'Adreslijst...' hebt geselecteerd, verschijnt het eerste scherm van de 'Wizard internet-verbindingen'.



Figuur 68: Wizard internet-verbinding, Naam van internet-adreslijstserver

Stap 1: servernaam invoeren

- Voer in het veld ‘internet-adreslijstserver (LDAP)’ het adres van server in: ‘`ldap.kennisnet.nl`’ server.
- Klik op de knop ‘Volgende>’.



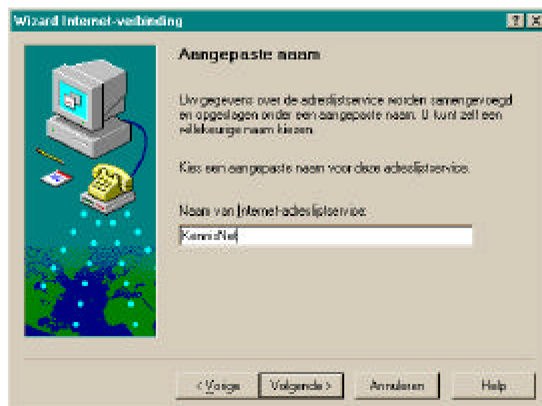
Figuur 69: Wizard internet-verbinding, E-mailadressen controleren

Stap 2: e-mailadressen controleren

In het tweede venster wordt gevraagd of u de LDAP-server wilt gebruiken om e-mailadressen te controleren aan de hand van een naam. Wanneer u bij het verzenden van een bericht een persoonsnaam intypt, controleert Outlook uw adressenboek. Als u hier het keuzerondje ‘Ja’ selecteert, controleert Outlook ook de LDAP-server op het voorkomen van de betreffende naam.

Het opzoeken van de naam in de LDAP-server kan vertragend werken. U kunt het beste het keuzerondje ‘Nee’ selecteren.

- Klik nadat u uw keuze hebt gemaakt op de knop ‘Volgende>’.



Figuur 70: Wizard internet-verbinding, Aangepaste naam

Stap 3: omschrijving account

- Voer in het veld 'Naam van internet-adreslijstservice' een naam naar keuze in (bijvoorbeeld: KennisNet).
- Klik op de knop 'Volgende>'.



Figuur 71: Wizard internet-verbinding, Voltooien

Stap 4: voltooien

- Klik op de knop 'Voltooien' om de instellingen op te slaan.

U kunt nu zoeken op personen op kennisnet.

5.4 Ik heb een webbrowser die ik niet automatisch kan instellen voor kennisnet?

In dit geval moet u kiezen voor handmatige instelling van de proxy-configuratie.

- Voer onder de instellingen van uw webbrowser het adres van de proxy-server van kennisnet in: '`proxy.kennisnet.nl`'.
- Voer tevens het poortnummer in: 8080.

Indien uw bladerprogramma helemaal geen proxy-configuratie ondersteunt, dient u over te stappen op een andere webbrowser.

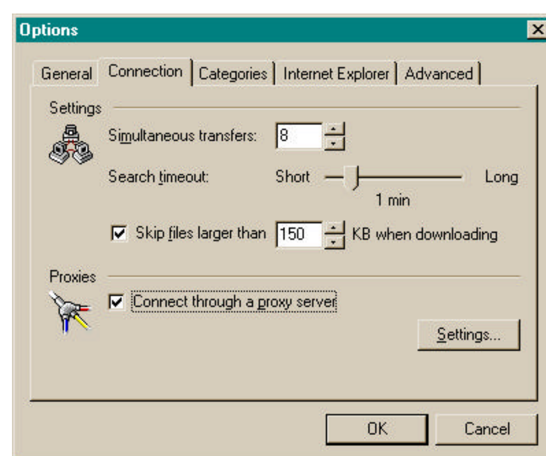
5.5 Zoeken op kennisnet: Copernic

Naast de gebruikelijke zoekmachines zoals Yahoo, Altavista of Ilse, bestaan er ook zogenoemde meta-zoekmachines zoals Copernic. Copernic combineert tijdens het zoeken een aantal zoekmachines en heeft dus een groter bereik dan een enkele zoekmachine. U kunt Copernic ook gebruiken om te zoeken op kennisnet.

Volg de volgende procedure om de instellingen voor kennisnet in Copernic in te voeren.

- Open Copernic.
- Kies uit het menu 'View' de optie 'Options'.
- Selecteer vervolgens het tabblad 'Connection'.

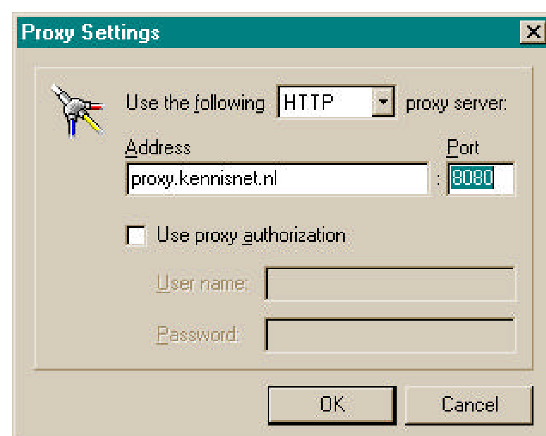
Het tabblad 'Connection' wordt geopend.



Figuur 72: Copernic: Options, Connection

- Selecteer het aanvinkvakje 'Connect through a proxy server'.
- Klik vervolgens op de knop 'Settings...'

Het venster 'Proxy Settings' wordt geopend.



Figuur 73: Copernic: Proxy Settings

In de keuzelijst staat standaard 'HTTP'. Dit dient u zo te laten.

- Voer in het veld 'Address' het adres van de proxy-server in: '`proxy.kennisnet.nl`'.

- Voer in het veld ‘Port’ het poortnummer in: 8080.
- Klik op de knop ‘OK’ om terug te keren naar het tabblad ‘Connection’.
- Klik vervolgens op de knop ‘OK’ om de instellingen op te slaan.

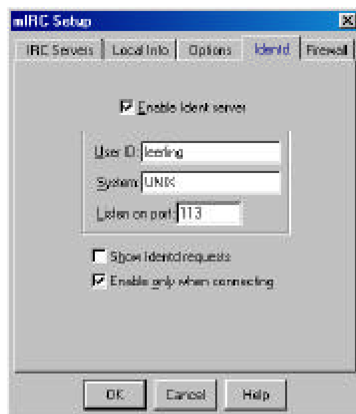
U kunt Copernic nu gebruiken om te zoeken op kennisnet.

5.6 Chatten op internet en kennisnet: Internet Relay Chat (IRC)

Met Internet Relay Chat kunt u onder meer chatten op het internet. Een bekend programma voor IRC is mIRC. Dit programma is geschikt om via de proxy-server van kennisnet met anderen op het internet te communiceren. Wanneer u van IRC gebruik wilt maken moet u de instellingen voor kennisnet invoeren in mIRC.

Volg de volgende procedure om de kennisnetinstellingen in mIRC in te voeren.

- Start mIRC.
- Open het venster ‘mIRC Setup’.
- Selecteer het tabblad ‘Identd’.



Figuur 74: mIRC Setup, Identd

Sommige IRC-servers op het internet stellen er prijs op dat de gebruikers zich via de optie ‘identd’ legitimeren. Het kan nuttig zijn om deze optie in te schakelen.

- Voer in het veld ‘User ID’ een gebruikersnaam in.

De overige instellingen kunt u ongemoeid laten.

- Selecteer vervolgens het tabblad ‘Firewall’.



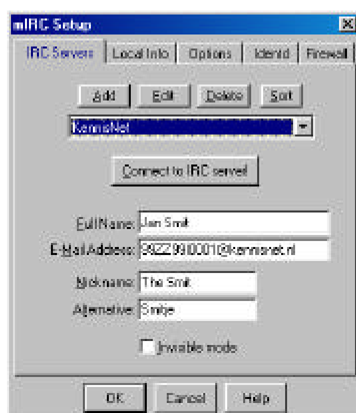
Figuur 75: mIRC Setup, Firewall

Om via internetservers buiten kennisnet met anderen te kunnen communiceren, is het noodzakelijk dat ondersteuning voor de socks-proxy [7] wordt ingesteld.

- Selecteer het aanvinkvakje ‘Use SOCKS Firewall’.
- Selecteer het aanvinkvakje Socks4.
- Voer in het veld ‘Hostname’ het adres van de socks-proxy-server in: ‘`socks-proxy.kennisnet.nl`’.
- Voer in het veld ‘Poort’ het poortnummer in: 1080.

De overige instellingen kunt u ongemoeid laten.

- Selecteer vervolgens het tabblad ‘IRC Servers’.



Figuur 76: mIRCSetup, IRC Servers

Op het tabblad ‘IRC Servers’ kunt u servers selecteren (of toevoegen) die u wilt gebruiken om te communiceren op het internet. Er is al een grote lijst met servers voorgeprogrammeerd waaruit kan worden gekozen. U kunt hier ook uw identiteit invoeren.

- Voer in het veld ‘E-Mail Address’ uw e-mailadres in (gebruikersnaam@kennisnet.nl).
- Voer in het veld ‘Nickname’ een willekeurig pseudoniem in waaronder u bekend wilt staan.

---

[7] Zie ook deel I en deel VII voor uitleg van het begrip ‘proxy’ en de beveiliging van proxy-servers. SOCKS is een protocol dat aan bepaalde andere op internet gebruikte protocollen toegang biedt tot diensten die zich buiten het lokale netwerk en achter de firewall bevinden.

De overige velden zijn niet verplicht.

- Klik op de knop 'OK' om de instellingen op te slaan.

U kunt nu met mIRC chatten op internet.

5.7 Bestanden up- en downloaden: File Transfer Protcol (FTP)

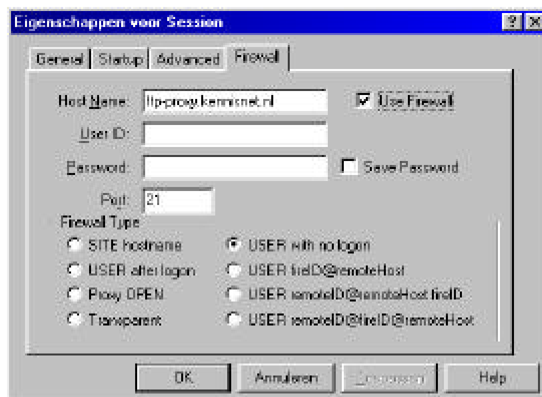
U kunt op kennisnet op een aantal manieren bestanden downloaden. Zo kunt u met uw webbrowser naar een website surfen en daar bestanden downloaden. FTP is een andere manier om bestanden te downloaden. Een voordeel van FTP is dat u er ook bestanden mee kunt uploaden. Wanneer u bijvoorbeeld een website voor uw school hebt gemaakt, kunt u deze met een FTP-programma op de voor uw school gereserveerde ruimte op de kennisnetserver zetten.

Hieronder worden de kennisnetinstellingen van twee FTP-programma's beschreven: WS-FTP lite voor de pc en Transport/Transmit voor de Apple Macintosh. Dit is maar een greep uit de FTP-programma's die in de omloop zijn. In paragraaf 5.12 kunt u lezen waar u nog meer 'gratis' FTP-programma's kunt downloaden.

5.7.1 WS-FTP lite

Volg de volgende procedure om de kennisnetinstellingen in WS-FTP lite in te voeren.

- Start WS-FTP lite.
- Klik op de knop 'Connect' (verbinden).
- Selecteer het tabblad 'Firewall'.



Figuur 77: WS FTP lite edition: Eigenschappen voor Session, Firewall

- Voer in het veld 'Host Name:' het adres van de FTP-proxy-serrver in: '`ftp-proxy.kennisnet.nl`'.
- Voer in het veld 'Port:' het poortnummer in: 21.
- Activeer de firewall door het aanvinkvakje 'Use Firewall' te selecteren.
- Selecteer onder 'Firewall Type' het keuzerondje 'USER with no logon'
- Klik op de knop 'OK'.
- Selecteer vervolgens het tabblad 'General'

Hier kunt u de overige gegevens voor de verbinding invoeren (bestemming, gebruikersnaam op de andere machine, enz.).

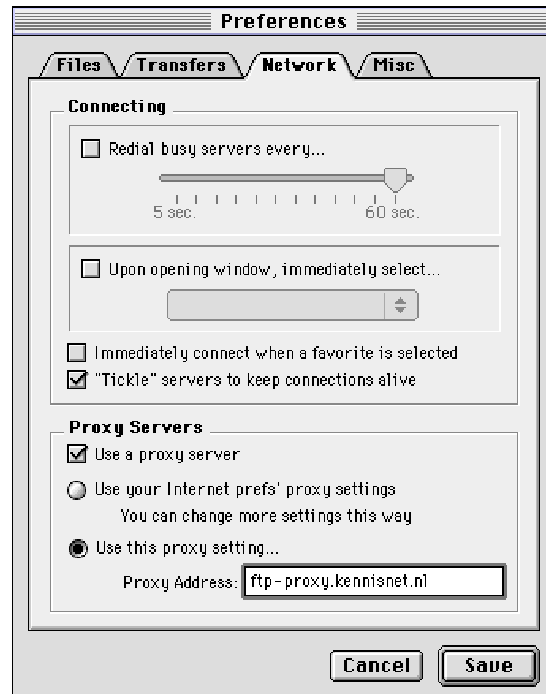
Let op!

Iedere keer wanneer u WS-FTP Lite opnieuw opstart, moet u deze handeling herhalen.

5.7.2 Transport/Transmit (Macintosh)

Volg de volgende procedure om de kennisnetinstellingen voor Transport/Transmit in te voeren.

- Kies uit het menu ‘Edit’ de optie ‘Preferences’.
- Selecteer het tabblad ‘Network’.



Figuur 78: Preferences, Network

- Selecteer onder ‘Proxy Servers’ het aanvinkvakje ‘Use a proxy server’.
- Selecteer het keuzerondje ‘Use this proxy setting...’.
- Voer in het veld ‘Proxy Address’ het adres van de proxy-server in: ‘`ftp-proxy.kennisnet.nl`’.
- Klik op de knop ‘Save’ om de instellingen te bewaren..

Transport/Transport is klaar voor gebruik.

5.8 Naar internet telnetten

U kunt naar internet telnetten, mits u een telnetprogramma hebt dat de SOCKS-firewall ondersteunt. Hieronder wordt een aantal van dergelijke telnetprogramma’s besproken.

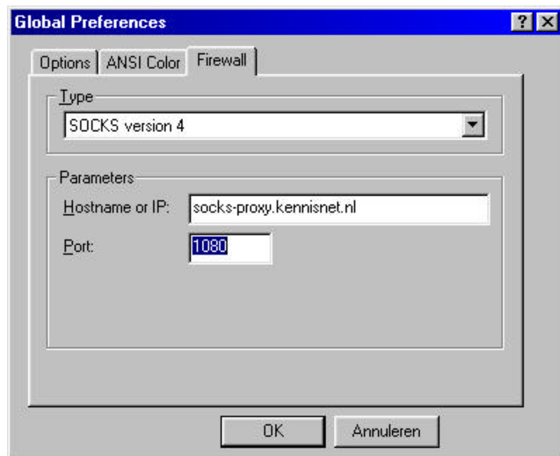
Een andere ‘truc’ (alleen voor Windows) is om gebruik te maken van SocksCap. Dit is een stukje programmatuur dat het IP-netwerkverkeer opvangt, voorzover het via de firewall zou moeten lopen, en omleidt. Zie paragraaf 5.8.3.

5.8.1 CRT (Windows)

Eén van de telnetprogramma’s die SOCKS ondersteunt, is CRT. Om het programma in te stellen voor het gebruik van de firewall, moet u de ‘Global Preferences’ aanpassen.

- Selecteer uit het menu ‘Options’ de optie ‘Global Preferences’.
- Ga naar het tabblad ‘Firewall’.

Het volgende venster verschijnt.



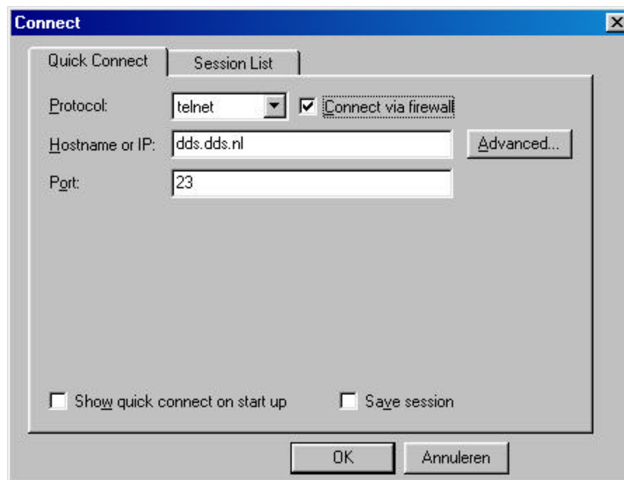
Figuur 79: CRT: Global Preferences, Firewall

- Selecteer uit de keuzelijst 'Type' het type "SOCKS version 4" of "SOCKS version 5 (no authentication)".
- Voer in het veld 'Hostname or IP:' in: "`socks-proxy.kennisnet.nl`".
- Voer in het veld 'Port:' het poortnummer in: "`1080`".
- Klik op de knop 'OK'.

Wanneer u een verbinding wilt opzetten, dient u expliciet aan te geven dat u gebruik wilt maken van de SOCKS-firewall.

- Selecteer bij 'Connect' het tabblad 'Quick Connect'.

Het volgende venster verschijnt, waarmee u de instellingen voor een verbinding kunt ingeven.



Figuur 80: CRT: Connect, Quick Connect

- Selecteer het aanvinkvakje 'Connect via firewall'.
- Voer in het veld 'Hostname or IP:' en in het veld 'Port:' respectievelijk het adres van de machine en het poortnummer in, waar u naar wilt telnetten.
- Klik op de knop 'OK'.

De verbinding wordt opgezet.

5.8.2 Mocha Telnet (Java)

De Java-versie van Mocha Telnet (http://www.mochasoft.dk/java.html#telnet[8]) ondersteunt SOCKS4. Om gebruik te maken van de SOCKS-proxy van kennisnet, dient u het bestand ‘`telnet2.html`’ dat bij het pakket zit, te wijzigen, dat wil zeggen: enkele parameters voor het Java-applet toe te voegen. Hieronder is de code voor het HTML-bestand gegeven:

```
<HTML>
<HEAD>
<TITLE> Mocha Telnet </TITLE>
</HEAD>
<BODY>
<APPLET CODE="telnet.class" WIDTH=1 HEIGHT=1>
<param name=type value="frame">
<param name=screen_x value="100">
<param name=screen_y value="100">
<param name=screen_width value=600>
<param name=screen_height value=500>
<param name=proxy_host value="socks-proxy.kennisnet.nl">
<param name=proxy_port value=1080>
<param name=proxy_socks value=true>
</APPLET>
</BODY>
</HTML>
```

Figuur 81: HTML-code voor proxyconfiguratie van Mocha Telnet

Omdat het een Java-applet betreft, kan het programma in principe op ieder type computer werken waarvoor Java wordt ondersteund. Indien uw internet-browser (bladerprogramma voor internet) de mogelijkheid biedt om netwerkbeveiligingen (tijdelijk) uit te schakelen voor Java, kunt u het programma starten door met uw bladerprogramma het bovenstaande HTML-bestand te openen.

Een andere optie is om de ‘appletviewer’ van de Java Development Kit of de Java Runtime Environment te gebruiken[9].

In Figuur 83 is een voorbeeld getoond van Mocha Telnet, uitgevoerd door de ‘appletviewer’ onder Linux. Ditzelfde kunt u ook onder Windows of op een Macintosh. Voor Windows kunt u een kort ‘batch’-bestand (script) maken, dat met de appletviewer het telnetprogramma start. Noem dit bestand bijvoorbeeld ‘MTELNET.BAT’, zie Figuur 82. U kunt eenvoudig een icoontje maken om het programma te starten.

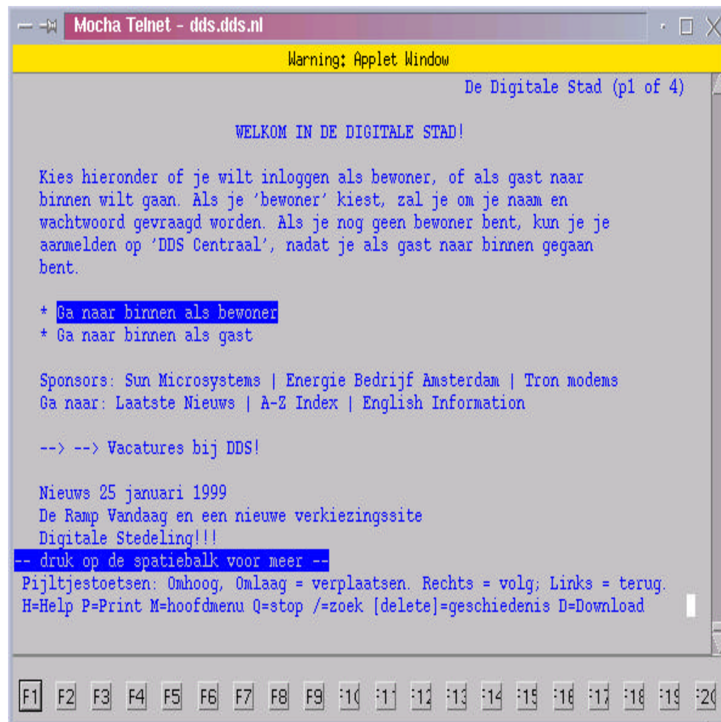
```
%ECHO OFF
APPLETVIEWER telnet2.html
```

Figuur 82: MTELNET.BAT

[8] Op dit adres kunt u een demonstratieversie ophalen; voor het volledige programma dient u te betalen.

[9] De Java Development Kit of Java Runtime Environment kunt u ophalen bij JavaSoft: http://www.javasoft.com/products/index.html. Kies het voor u geschikte platform, eventueel kunt u kijken bij ‘ports’ voor *uw* besturingssysteem.

Informatie over het starten van Java-applets onder Mac OS kunt u vinden op het adres http://developer.apple.com/techpubs/java/MacOSandJava/JManager/JManager2.1/JManager.21.html.



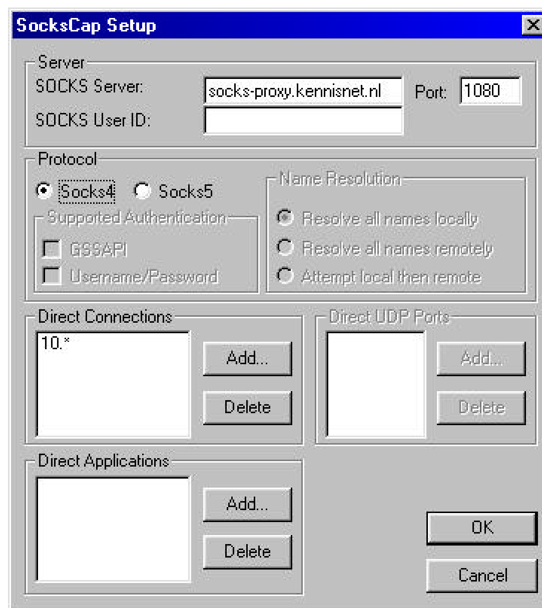
Figuur 83: Mocha Telnet voor Java tm

5.8.3 SocksCap

Met SocksCap (Windows) kunt u individuele programma's door een 'SOCKS'-firewall loodsen, wanneer zij gebruikmaken van protocollen die door SOCKS worden ondersteund. Telnet van Windows en TeraTerm werken hier in ieder geval mee samen. U kunt SocksCap ophalen van de website http://www.socks.nec.com/. U kunt kiezen uit een versie voor Windows 3.x (16 bit) en Windows 95/98/NT (32 bit).

- Kies uit het menu 'File' de optie 'Setup'.

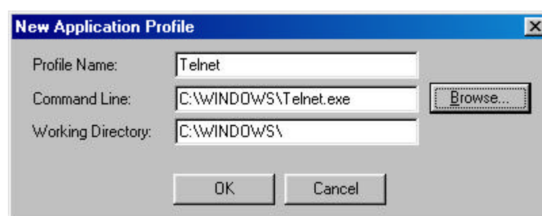
Het volgende venster verschijnt.



Figuur 84: SocksCap Setup

- Voer in het veld ‘SOCKS Server:’ in “`socks-proxy.kennisnet.nl`”.
- Voer in het veld ‘Port:’ in: het getal “1080”.
- Maak het veld ‘SOCKS User ID:’ leeg.
- Selecteer voor het protocol het keuzerondje ‘Socks5’.
- Selecteer onder ‘Name Resolution’ het keuzerondje ‘Resolve all names locally’
- Bij ‘Direct Connections’ klikt u op de knop ‘Add...’.
- In het selectieblok dat dan verschijnt, voert u “`10.*`” in.
- Klik op de knop ‘OK’ om het venster te sluiten.

Vervolgens dient u applicaties in te stellen voor het gebruik van SocksCap. Als voorbeeld is in Figuur 85 de instelling afgebeeld voor Telnet.exe, dat standaard bij Windows 95/98/NT wordt geleverd.



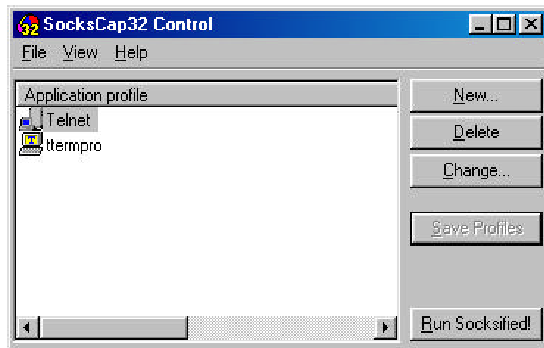
Figuur 85: SocksCap: New Application Profile

- Zoek met de knop ‘Browse...’ het programma op dat u via SOCKS wilt gebruiken.

De meeste gegevens worden direct ingevuld, eventueel kunt u de titel (in het veld ‘Profile Name:’) nog aanpassen.

- Klik op de knop ‘OK’ om het venster te sluiten.

U komt terug in het hoofdvenster.



Figuur 86: SocksCap32 Control: hoofdvenster

- Klik op de knop ‘Save Profiles’ om de instellingen te bewaren.

Daarmee bent u klaar om te werken.

- Klik op de knop ‘Run Socksified’ om een programma met SocksCap te starten.

Hierdoor zal SocksCap een aantal systeemfuncties omleiden en uw programma zal, waar mogelijk, via de SOCKS-firewall naar het internet worden geleid.

Let op!

SocksCap werkt niet voor alle TCP/IP-programmatuur. Controleer dit om teleurstellingen te voorkomen.

5.9 RealAudio of RealVideo gebruiken

U kunt RealAudio of RealVideo gebruiken. Zie ook deel IV.

Maar het probleem is dat er in het verleden diverse verschillende protocollen zijn gebruikt voor het transporteren van ‘Real’ data. Niet voor alle protocollen zijn er mogelijkheden om deze op een nette manier door een firewall heen te transporteren. Vanaf de versie ‘G2’ van de RealPlayer is het mogelijk om gebruik te maken van het ‘RTSP’, ‘RealTime Streaming Protocol’. Een voorwaarde is echter weer, dat ook de server die de uitzending moet verzorgen, dit protocol ondersteunt. Voor dit protocol is een proxy -voorziening getroffen op `rtsp-proxy`, poort 554.

Een andere optie is het gebruik van HTTP, het protocol dat ook wordt gebruikt voor het versturen van webpagina’s tussen webservers en bladerprogramma’s. Dit protocol is echter niet ontworpen voor het communiceren van ‘streaming data’ (een voortdurende stroom gegevens) en servers zitten snel aan hun maximale capaciteit qua aantallen verbindingen.

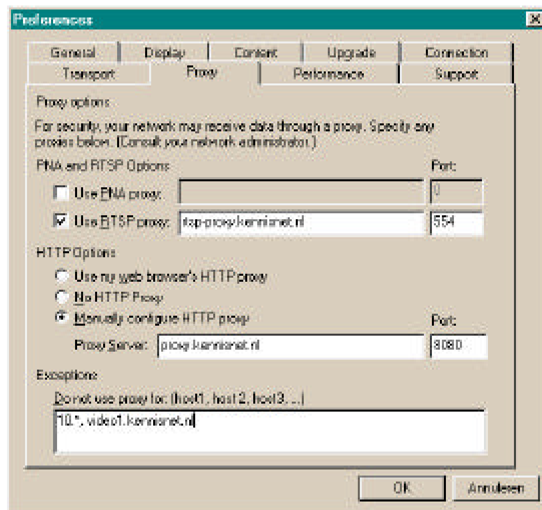
Om de instellingen in de RealPlayer G2 te kunnen aanpassen voor kennisnet, kunt u in het programma zelf de optie ‘Preferences’ uit het menu ‘Options’ kiezen. Hiervoor dient het venster ‘groot’ te zijn, anders is het menu niet compleet. U kunt het venster ‘groot’ maken door op de knop helemaal rechts te klikken, zoals met de cirkel aangegeven in het volgende venster.



Figuur 87: RealPlayer klein

Een andere manier is om in het configuratiescherm van Windows de instellingen voor RealPlayer G2 te selecteren.

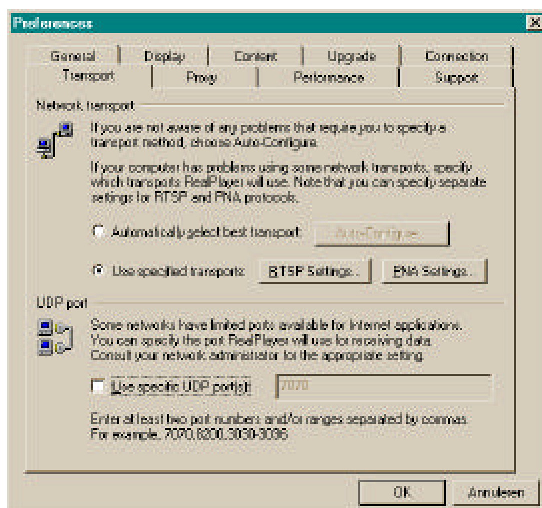
- Ga naar het tabblad ‘Proxy’.



Figuur 88: Preferences, Proxy

- Selecteer *alleen maar* het aanvinkvakje 'Use RTSP-proxy'.
- Voer achter 'Use RTSP-proxy' als machinenaam '`rtsp-proxy.kennisnet.nl`' in en als poort voert u "`554`" in.
- Om dezelfde proxy als uw internet-browser (bladerprogramma voor internet) te gebruiken: selecteer onder 'HTTP Options' het keuzerondje 'Use my web browser's HTTP proxy'.
- Mogelijk is het beter om de instellingen met de hand in te geven: selecteer dan het keuzerondje 'Manually configure HTTP proxy'. Voer dan in het veld 'Proxy Server" in "`proxy.kennisnet.nl`" (*let op:* dus zonder nummer!) en in het veld 'Port' het getal "`8080`".
- Onder 'Exceptions' moet u in het veld 'Do not use proxy for: (host1, host2, host3, ...)' aangeven welke adressen *niet* via de proxy moeten gaan. Voer in: "`10.*, 127.*`".

Op het tabblad 'Transport' (zie Figuur 89) kunt u de manier aangeven waarop bij voorkeur gegevens worden overgedragen.

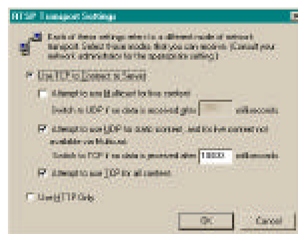


Figuur 89: Preferences, Transport

Standaard zal het programma, zo mogelijk automatisch, proberen om de beste manier van gegevenstransport te selecteren. Helaas slaagt het programma er niet altijd in. In dat geval zult u het met de hand moeten instellen:

- Selecteer voor de handmatige instelling het keuzerondje 'Use specified transports:'.
- Met de knoppen 'RTSP Settings…' (zie Figuur 90) en 'PNA Settings...' (zie Figuur 91) kunnen de instellingen voor verschillende protocollen worden aangegeven.

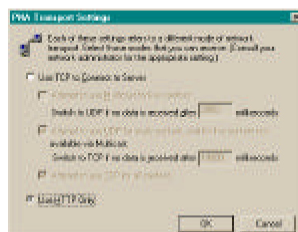
Met de knop 'RTSP Settings...' (zie Figuur 89) verschijnt het volgende venster.



Figuur 90: RTSP Transport Settings

- Selecteer het keuzerondje 'Use TCP to Connect to Server'.
- Het aanvinkvakje bij de eerste suboptie kunt u beter *niet* selecteren, de beide anderen wel.
- Klik op de knop 'OK'.

Met de knop 'PNA Settings...' (zie Figuur 89) verschijnt het volgende venster:



Figuur 91: PNA Transport Settings

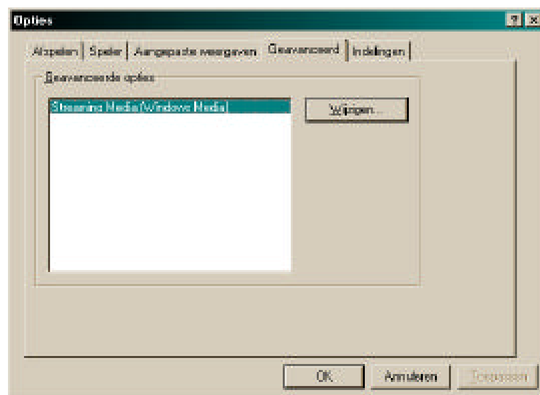
- Selecteer het keuzerondje 'Use HTTP Only'.
- Klik op de knop 'OK'.

5.10 Windows Media Player gebruiken

Om met de Windows Media Player (die overigens ook voor Mac OS beschikbaar is) mediabestanden te kunnen afspelen, dient u uitsluitend van HTTP gebruik te maken. Het Microsoft-specifieke protocol voor de Media Player wordt *niet* ondersteund door de proxy's van kennisnet.

- Kies uit het menu 'Beeld' en dan 'Opties'.

Er verschijnt een venster. Ga naar het tabblad 'Geavanceerd'.

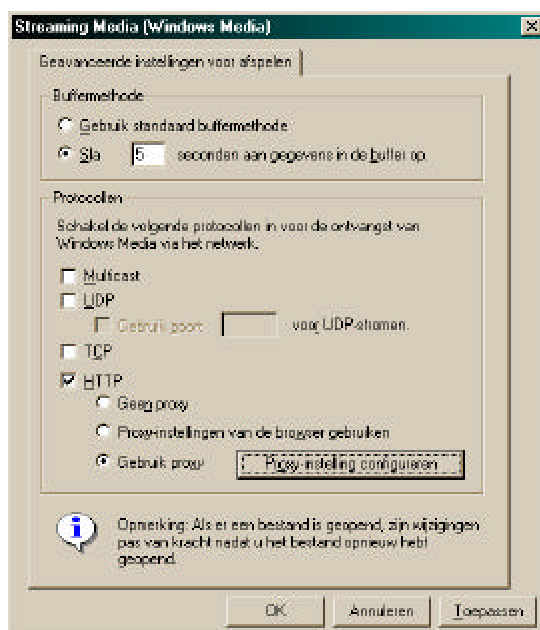


Figuur 92: Opties, Geavanceerd

Op dit tabblad staat onder 'Geavanceerde opties' een selectieblok met ondersteunde mediatypen.

- Selecteer 'Streaming Media (Windows Media)'.
- Klik op de knop 'Wijzigen...'.

Het volgende venster verschijnt.



Figuur 93: Streaming Media, Geavanceerde instellingen voor afspelen

- Selecteer onder 'Protocollen' *alleen maar* het aanvinkvakje 'HTTP'.
- Selecteer bij 'HTTP' hetzij het keuzerondje 'Proxy -instellingen van de browser gebruiken', hetzij het keuzerondje 'Gebruik proxy'.

  In het laatste geval dient u het adres van de proxy in te stellen:

  - Klik op de knop 'Proxy -instelling configureren'.

Het volgende venster verschijnt.



Figuur 94: Streaming Media, naam en port van Proxy

- Voer in het veld ‘Naam’ in: “proxy.kennisnet.nl”, en in het veld ‘Poort’: “8080”.
- Klik op de knop ‘OK’.
- Sluit het venster van Figuur 93 met de knop ‘Toepassen’.
- Sluit het venster van Figuur 92 met de knop ‘OK’.

5.11 De klok van de computers automatisch goed zetten

Kennisnet heeft zogenoemde tijdservers, die u kunt gebruiken om de systeemklok van uw computers te synchroniseren. Deze tijdservers zijn te bereiken via het internetadres `time.kennisnet.nl` en kunnen via het SNTP-protocol (Simple Network Time Protocol) worden benaderd. Er bestaan diverse hulpprogrammaatjes – commercieel, shareware en gratis – die u kunt gebruiken om de systeemklokken goed te zetten en bijvoorbeeld bij het opstarten van uw computer in de achtergrond te starten.

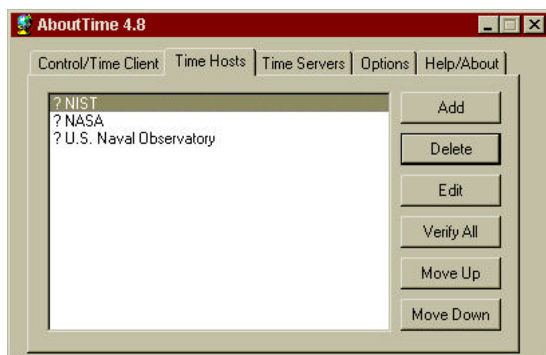
Echter, wanneer iedereen op kennisnet gebruik gaat maken van dezelfde tijdservers, zal dit ernstige gevolgen hebben voor de prestaties van deze machines. Het wordt daarom aangeraden om lokaal een eigen tijdserver op te zetten en die periodiek (bijvoorbeeld eens per dag) te laten synchroniseren met de centrale tijdservers. U kunt bijvoorbeeld op uw lokale netwerkserver een extra proces starten.

5.11.1 AboutTime

AboutTime is een klein, doch handig programmaatje voor het gelijkzetten van de tijd van lokale pc’s. Het kan zowel client als server zijn. Hier volgt enige uitleg van de bediening van AboutTime op kennisnet.

Wanneer u AboutTime voor de eerste keer start, dient u nog enkele instellingen aan te passen voor de situatie op kennisnet. De standaard ingestelde servers zijn namelijk niet rechtstreeks bereikbaar op kennisnet.

- Ga naar het tabblad ‘Time Hosts’.



Figuur 95: AboutTime, Time Hosts

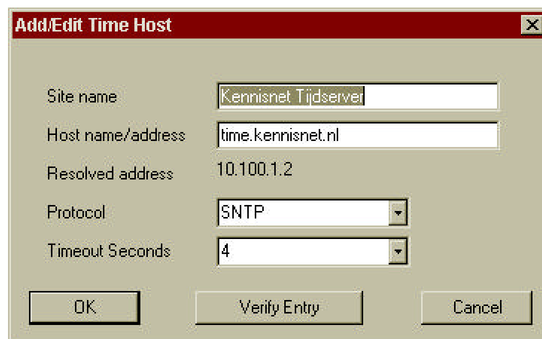
Hier staan reeds drie timeservers aangegeven.

- Verwijder deze servers met de knop ‘Delete’.

Vervolgens dient u de servers van kennisnet eraan toe te voegen.

- Klik op de knop ‘Add’ om de opties voor de timeservers in te vullen.

Het volgende venster verschijnt.



Figuur 96: Add/Edit Time Host

- Voer in het veld ‘Site name’ een omschrijving van de timeserver in, bijvoorbeeld ‘Kennisnet Tijdserver’.
- Voer in het veld ‘Host name/address’ het internet-adres van de timeserver in: “`time.kennisnet.nl`”.
- Voer in of selecteer uit de keuzelijst bij ‘Protocol’ “SNTP” (dit is de standaard).
- Voer in of selecteer uit de keuzelijst bij ‘Timeout Seconds’: ‘4’ seconden (dit is standaard).
- U kunt controleren of de host bes taat: klik op de knop ‘Verify Entry’.

  Let op!

  Deze knop stelt u níet in staat om te testen of AboutTime correct werkt.

Indien de host niet bestaat of niet gevonden kan worden, krijgt u een foutmelding. Oorzaken kunnen zijn:

- DNS-probleem;
- geen verbinding;
- time-out.

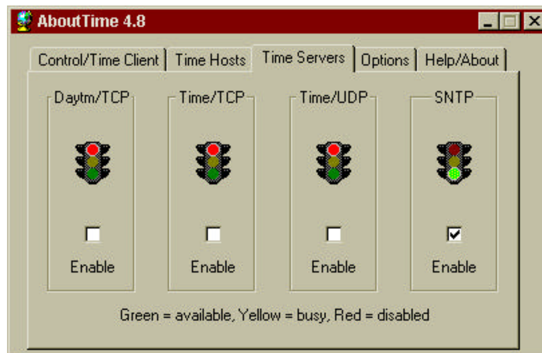
U krijgt bijvoorbeeld een bericht als het volgende.



Figuur 97: Verify host name/address: Unable to verify

Wanneer u uw lijst van timeservers hebt ingevoerd, kunt u in Figuur 95 eventueel nog de volgorde bepalen met de knoppen ‘Move up’ en ‘Move down’.

Zoals gezegd kan AboutTime ook als server optreden. Ga voor de instellingen hiervoor naar het tabblad ‘Time Servers’.



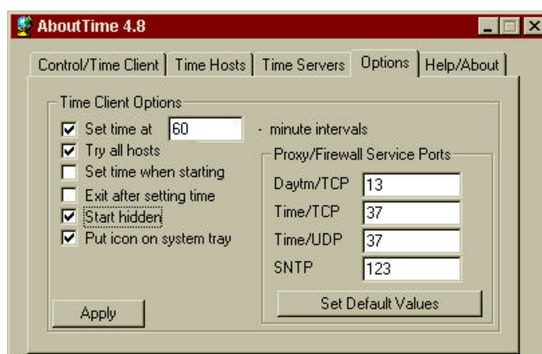
Figuur 98: AboutTime, Time Servers

Hier staat een viertal verkeerslichtjes met een aanvinkvakje eronder.

- Door een aanvinkvakje te selecteren, zet u het verkeerslicht op groen en wordt de bijbehorende service actief. Elk van de verkeerslichtjes vertegenwoordigt een protocol om de tijd uit te wisselen. Standaard staan alle protocollen aan.

  Let op!

  Het verdient aanbeveling om slechts één of twee machines in uw lokale netwerk aan de centrale server te laten refereren. De rest van de computers kan gebruikmaken van uw lokale systemen.
- Ga ten slotte naar het tabblad ‘Options’.



Figuur 99: AboutTime, Options

Hier kunt u een aantal resterende instellingen invullen.

- Het kan nuttig zijn om het aanvinkvakje ‘Start hidden’ te selecteren; hiermee wordt het programma onzichtbaar gestart.
- Door het aanvinkvakje ‘Put icon on system tray’ ook te selecteren (standaard), is het icoontje wel zichtbaar in de systeembalk, normaliter rechts onder in het beeld.
- Het interval tussen het verversen van de tijd (aanvinkvakje en veld ‘Set time at’) staat standaard ingesteld op 60 minuten. Deze tijd kunt u voor een lokale server gerust op een dag (= 60 maal 24 = 1440 minuten) instellen.
- Met name voor lokale werkstations kan het aanvinkvakje ‘Set time when starting’ zinvol zijn om de tijd direct gelijk te zetten bij het opstarten van de pc of de sessie.

Ga eventueel naar het eerste tabblad om met de knop ‘Hide’ het venster te verbergen.

Om ‘AboutTime’ altijd bij het aanmelden op het systeem te starten, kunt u een snelkoppeling in de groep ‘Opstarten’ van het Startmenu plaatsen.

5.12 Internetadressen om software te krijgen of te kopen

Veel van de genoemde software is zonder problemen op internet te vinden. De genoemde internet-browsers (bladerprogramma's voor internet) zijn vrij verkrijgbaar via de producenten van de software.

Zo kunt u de nieuwste versie van Microsoft Internet Explorer vinden op de website van Microsoft: http://www.microsoft.com/.

Netscape Communicator kunt u vinden op de website van Netscape Communications: http://home.netscape.com/, maar ook op vele andere websites en FTP-sites.

De meest genoemde FTP-software is op te halen van 'Tucows': http://tucows.a2000.nl/ of http://www.tucows.com/. Kies in het hoofdmenu het gewenste software- en hardwareplatform en zoek de gewenste programmatuur.

Andere bekende bronnen van software zijn http://www.download.com/ en http://www.software.com/.

AboutTime kunt u verkrijgen op http://www.arachnoid.com/.

Let op 1!

Niet alle software is gratis! Bepaalde producten kunt u maar voor een beperkte periode uitproberen, voordat u betaalt. Andere software heeft enkele functionaliteiten die pas worden ingeschakeld als u zich hebt geregistreerd en voor de software hebt betaald. Ook bij producten die als 'freeware' (gratis software) worden aangeboden, kan er een 'addertje onder het gras' zitten, bijvoorbeeld omdat de software slechts onder bepaalde omstandigheden of voor een beperkte doelgroep gratis is: meestal thuisgebruikers of educatieve instellingen. Ook mag u gratis software niet altijd verder verspreiden.

Lees dus altijd de licentievoorwaarden voordat u de software gaat gebruiken!

Let op 2!

internet is een tamelijk onveilig medium als het gaat om softwaredistributie. Wees zeer zorgvuldig in het gebruik van software die van internet afkomstig is, zeker als het om onbekende websites of FTP-sites gaat.

Controleer uw software daarom altijd vóór gebruik op mogelijke virusinfecties!

5.13 Thuis gebruikmaken van kennisnet-diensten

Uiteraard dient u om thuis gebruik te maken van kennisnet-diensten een verbinding te hebben met internet via een andere internetaanbieder dan kennisnet. Raadpleeg deze aanbieder voor alle informatie over hoe u verbinding dient te maken met internet en hoe u via deze aanbieder kunt surfen.

De diensten van kennisnet die u *buiten* kennisnet kunt gebruiken, zijn voornamelijk het lezen van uw elektronische post (e-mail) en in beperkte mate het raadplegen van informatie op kennisnet. Raadpleeg deel IV voor Kennisnet Webmail, waarmee het overal ter wereld mogelijk is via internet-browsers te e-mailen met het mailadres van kennisnet.

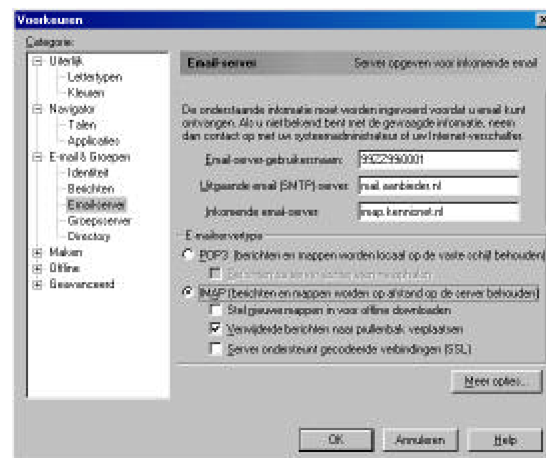
5.13.1 Thuis e-mail lezen en versturen

Om thuis uw e-mail te lezen, dient u dezelfde instellingen te gebruiken als op kennisnet zelf, *behalve* voor uw uitgaande post. Om te voorkomen dat er misbruik wordt gemaakt van de mailvoorzieningen van kennisnet, zijn er speciale filters aangebracht. Deze hebben echter ook tot gevolg dat u niet van buiten kennisnet post naar buiten kennisnet kunt verzenden. U dient daarom aan uw lokale internetaanbieder te vragen via welke machine u uw e-mail kunt verzenden.

Hieronder volgen uitgewerkte voorbeelden voor Netscape Communicator en Microsoft Outlook (Express). Hierbij wordt uitgegaan van de instellingen voor 'normaal' gebruik op kennisnet. In het voorbeeld wordt een denkbeeldige internetaanbieder "Aanbieder" gebruikt. Dit bedrijf heeft als server voor de uitgaande e-mailberichten een machine met de naam "`mail.aanbieder.nl`". De exacte gegevens voor uw situatie moet u uiteraard navragen bij *uw* eigen internetaanbieder.

In het geval dat u problemen ondervindt, zou u als uw *afzender*adres (het '`From:`'-veld in uw e-mail) het mailadres dat u van uw lokale aanbieder hebt gekregen, kunnen gebruiken, en als *antwoord*adres (het '`Reply-To:`'-veld in uw e-mail) uw kennisnetadres in kunnen vullen. In principe is dit vrijwel nooit nodig, maar sommige aanbieders controleren de informatie in berichtkoppen van uitgaande e-mailberichten op het '`From:`'-veld of dit binnen een door de aanbieder geaccepteerd domein valt. Een dergelijke controle wordt gedaan om 'SPAM' van binnenuit te voorkomen. Over 'SPAM' kunt u meer lezen in deel VII.

5.13.2 Netscape



Figuur 100: Voorkeuren, Categorie, E-mail & Groepen, E-mail-server

In Netscape Communicator stelt u de gegevens als volgt in. U kunt vrijwel alle instellingen overnemen uit de beschrijving in paragraaf 5.1.3:

- Selecteer de categorie 'E-mail & Groepen' en vervolgens subcategorie 'E-mail-server'.
- U dient hier uw gebruikersnaam in te voeren voor kennisnet. Voor de uitgaande e-mail vult u het adres van de mailserver van uw lokale internetaanbieder in; in dit voorbeeld "`mail.aanbieder.nl`". Voor de inkomende mail geeft u, afhankelijk van uw keuze voor POP3 of IMAP4, het adres "`pop.kennisnet.nl`", respectievelijk "`imap.kennisnet.nl`" op. Zie deel VI voor meer informatie over POP en IMAP.
- Onder subcategorie 'Identiteit' kunt u, indien nodig, het antwoordadres instellen.

Outlook (Express)



Figuur 101: Wizard *internet*-verbinding, E-mailservernamen

Tijdens het aanmaken van een e-mailaccount via de account-wizard krijgt u, zoals ook in paragraaf 5.3 is beschreven, een venster waarin u de mailserver opgeeft.

- Als server voor inkomende mail geeft u, afhankelijk van uw keuze voor het POP3-protocol of het IMAP4-protocol, de naam "`pop.kennisnet.nl`" respectievelijk "`imap.kennisnet.nl`".
- Voor uitgaande mail gebruikt u de server van uw aanbieder; in dit voorbeeld "`mail.aanbieder.nl`".

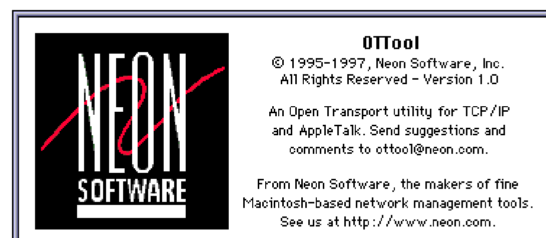
5.14 Handige software

Om eenvoudig bruikbare netwerkinformatie op te zoeken, zijn er wat handige hulpmiddelen beschikbaar op internet. Deze hulpmiddelen voor Mac OS en Windows zijn veelal een grafische afspiegeling van de UNIX-equivalenten die vanaf de commandoregel kunnen worden aangeroepen.

5.14.1 OTTool

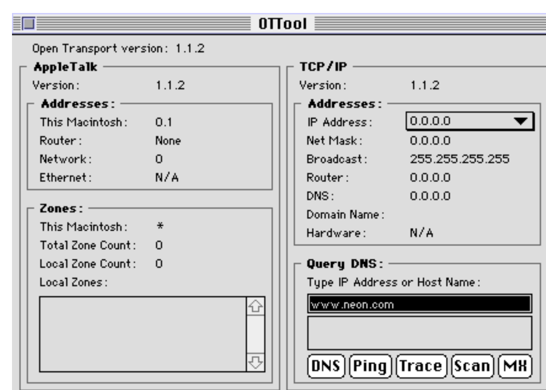
De *gratis* OTTool voor Mac OS is een stukje software dat informatie geeft over TCP/IP en AppleTalk. U kunt in één oogopslag uw AppleTalk-instellingen en TCP/IP-instellingen naast elkaar zien, waaronder het via DHCP verkregen IP-adres. Bovendien kunt u er IP-adressen en machinenamen op internet mee opzoeken en uitzoeken wat de mailserver ('MX') van een bepaald domein is.

U kunt OTTool ophalen van de site van Neon: http://www.neon.com/.



Figuur 102: OTTool-infovenster

Het hoofdvenster van OTTool ziet er zo uit:



Figuur 103: OTTool-hoofdvenster

- Met de knop 'DNS' kunt u het IP-adres of de machinenaam bij een gegeven machinenaam resp. IP-adres terugvinden.
- Met de knop 'Ping' kunt u kijken of de machine bereikbaar is. Let op: beveiligingsfilters kunnen ook de oorzaak van *geen reactie* zijn.

- Met de knop 'Trace' kunt u nagaan hoe het verkeer naar een bepaalde machine loopt.
- Met de knop 'Scan' kunt u zoeken naar andere machines in het netwerk.
- Met de knop 'MX' zoekt u voor een op te geven domein naar de mailmachines.

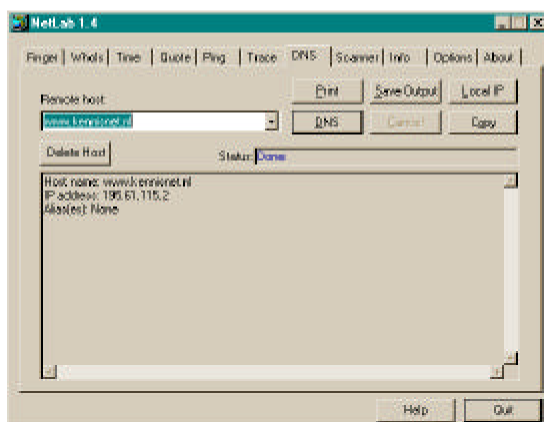
5.14.2 NetLab

Met NetLab voor Windows 95/98/NT kunt u, net als met OTTool, diverse netwerkdiensten raadplegen. NetLab is eigenlijk wat uitgebreider dan OTTool, op de DNS-functie na. U kunt namelijk geen mailmachine voor een domein opzoeken.

U kunt NetLab ophalen op het adres: ftp://ftp.worldonline.nl/pub/ZDNet/NETLAB.zip.

NetLab biedt, verdeeld over de verschillende tabbladen (zie Figuur 104), vele functies en uitgebreide informatie.

Met NetLab kunt u trouwens ook de klok van uw computer met andere computers synchroniseren via verschillende protocollen.



Figuur 104: NetLab, DNS

6. Netwerkadressen

In dit hoofdstuk worden twee veel voorkomende vragen behandeld met betrekking tot de te gebruiken netwerkadressen.

6.1 Welke adressen worden via DHCP uitgedeeld en welke kan ik zelf indelen?

De reeks adressen die een school krijgt toegewezen, kan in een aantal stukken worden opgedeeld:

- de router;
- één gereserveerd adres;
- werkplekken;
- lokale servers die vanaf kennisnet bereikbaar moeten zijn;
- lokale servers die niet vanaf kennisnet bereikbaar moeten zijn, en overige netwerkapparatuur.

De router heeft altijd het eerste adres uit de reeks.

6.2 Wat zijn de adressen van…

…de mailserver, newsserver enzovoort? Indien u van DHCP gebruikmaakt, wordt een deel van de adressen die u nodig hebt voor communicatie met kennisnet, automatisch ingevuld. Om gebruik te kunnen maken van e-mail, discussiegroepen (news), www en FTP, zijn echter nog speciale instellingen nodig.

Service	Naam of IP-adres	Poort
Mail versturen	smtp.kennisnet.nl	25
Mail ophalen	pop.kennisnet.nl	110
	imap.kennisnet.nl	143
Discussiegroepen	news.kennisnet.nl	119
Proxy [10]	proxy.kennisnet.nl	8080
Socks[11]	socks-proxy.kennisnet.nl	1080
RTSP-proxy (videoproxy)	rtsp-proxy.kennisnet.nl	554
RTSP-server (videoserver)	video.kennisnet.nl	554
FTP-proxy	ftp-proxy.kennisnet.nl	21
DNS	212.178.5.4	
	212.178.5.5	

Om de tijd van uw PC correct te laten lopen, kunt u ook gebruikmaken van de tijdservers van kennisnet. De proxy's beschikken beide over de juiste tijd en kunnen worden gebruikt om de klok van uw computers gelijk te zetten via het Network Time Protocol via het onderliggende Simple Network Time Protocol.

Service	Naam of IP-adres	Poort
Tijdserver	time.kennisnet.nl	(S)NTP

[10] Voor HTTP (www), 'beveiligd' (www), FTP, Gopher.

[11] Voor IRC, telnet.

7. Foutmeldingen

7.1 E-mail

7.1.1 Fouten tijdens de bezorging van e-mail

Nummer	Engelse melding	Nederlandse omschrijving
421	<*domein*> Service not available, closing transmission channel	Er is een probleem opgetreden of de dienst is tijdelijk niet beschikbaar (mogelijk voor onderhoud), waardoor het e-mailbericht niet kan worden afgeleverd op de betreffende machine.
450	Requested mail action not taken: mailbox unavailable	De postbus waar het bericht moet worden afgeleverd, kan op dit moment niet worden benaderd, mogelijk omdat het betreffende bestand op dit moment in gebruik is door een ander proces op de ontvangende machine.
451	Requested action aborted: local error in processing	Er is een (onbekende) fout opgetreden tijdens het verwerken van het bericht. Bijvoorbeeld omdat het ontvangende systeem niet correct is ingesteld.
452	Requested action not taken: insufficient system storage	Het bericht kon niet worden afgeleverd, omdat de opslagruimte op de ontvangende machine onvoldoende is. Mogelijk is uw bericht erg groot.
500	Syntax error, command unrecognized	Tijdens de communicatie tussen een zendende en een ontvangende machine is er een ongeldig commando aangeroepen, dat de ontvangende machine niet begrijpt. Dit kan duiden op een fout in de software in één van beide computers.
501	Syntax error in parameters or arguments	Een bepaald commando in de onderhandelingen tussen een verzendende en een ontvangende machine is aangeroepen met verkeerde parameters.
	<*e-mailadres*>... Sender domain must exist	Dit is één voorbeeld van een '501'-foutmelding. In dit geval wordt het e-mailadres van de ontvanger niet correct doorgegeven. Controleer of u uw e-mailadres, en met name het domein, correct hebt ingevuld in uw e-mailprogramma.
502	Command not implemented	Een aangeroepen commando is op de ontvangende machine niet geïmplementeerd en kan dus niet worden uitgevoerd. Wellicht betreft het een niet-standaard of niet-vereist commando voor correct functioneren. U zou deze fout eigenlijk niet mogen zien en mailservers moeten dit onderling oplossen.
503	Bad sequence of commands	De volgorde waarin tijdens de onderhandeling tussen een verzendende en een ontvangende machine commando's worden uitgevoerd, wordt door de ontvangende machine niet geaccepteerd. Dit duidt mogelijk op fouten in de software van de verzendende machine. Normaal zou de gebruiker deze melding niet mogen krijgen.

504	Command parameter not implemented	Een commando is tijdens de onderhandeling tussen een verzendende en een ontvangende machine aangeroepen met opties die niet door de ontvangende machine worden ondersteund.
550	Requested action not taken: mailbox unavailable	Het bericht kan niet worden afgeleverd, omdat de betreffende postbus niet beschikbaar is. Dit kan worden veroorzaakt doordat de postbus niet bestaat of doordat er onvoldoende rechten zijn om de postbus te openen en het bericht te plaatsen.
	<*e-mailadres*>... Relaying denied	Eén voorbeeld van de melding '550' is weigering van het doorzenden van e-mail. U probeert een bericht te bezorgen, waarvan noch de afzender, noch de ontvanger binnen een door de server geaccepteerd domein vallen. Zie ook deel VII.
551	User not local; please try <*ander adres*>	De gebruiker aan wie getracht wordt het bericht te zenden, is niet bekend op de betreffende machine. Er wordt mogelijk een alternatief adres gesuggereerd.
552	Requested mail action aborted: exceeded storage allocation	Het bericht kan (tijdelijk) niet worden bezorgd, omdat de postbus van de ontvanger vol is. Zodra de ontvanger zijn postbus opschoont, kan er weer post worden bezorgd. Controleer eventueel hoe groot het verzonden bericht is; indien dit bericht *echt* te groot is voor de ontvangende postbus, zult u het niet kunnen verzenden.
553	Requested action not taken: mailbox name not allowed	Het bericht kon niet worden bezorgd, omdat er een ongeldige naam voor de postbus is opgegeven. Controleer of het e-mailadres correct is ingevoerd.
554	Transaction failed	Het overzenden van het bericht tussen twee machines is niet gelukt. Controleer de inhoud van het foutbericht. Mogelijk hoeft het bericht (nog) *niet* opnieuw te worden verzonden, maar zal een tussengelegen machine nog enkele uren of zelfs dagen proberen om het bericht alsnog af te leveren.

7.1.2 Andere (fout)meldingen in de e-mail

Melding	**Betekenis**
Your mailbox has exceeded its size limit	U hebt teveel e-mail in uw postbus ('mailbox') staan. Probeer om oude berichten of berichten die u niet meer nodig hebt, weg te gooien om zo ruimte vrij te maken. Eventueel kunt u proberen om uw e-mail lokaal, d.w.z. op uw eigen computer of diskettes, op te slaan.
The following addresses had successful delivery notifications <*lijst met e-mailadressen*>	Er is niets aan de hand. U hebt waarschijnlijk om een ontvangstbevestiging gevraagd, welke u in dit bericht krijgt. In het bericht is een lijst gegeven met adressen waar het bericht met succes is afgeleverd.
Non-Delivery Report; Could not deliver message (ID=<*getal*>).	Het bericht dat u hebt verzonden, kon niet worden afgeleverd, bijvoorbeeld omdat de gebruikersnaam niet correct of onbekend is op het ontvangende systeem.

7.2 WWW

Hieronder volgt een lijst van bekende foutmeldingen die webservers kunnen geven, met hun betekenis.

Nummer	Engelse melding	Nederlandse omschrijving
300	Multiple Choices	De opgevraagde informatie is in verschillende representaties (formaten) beschikbaar. Er wordt een lijst gegeven van de verschillende representaties en het bijbehorende adres, zodat de gebruiker een keuze kan maken voor de gewenste representatie.
301	Moved Permanently	De opgevraagde informatie is verplaatst naar een nieuw adres. Verzoeken zouden in het vervolg naar één van de geretourneerde nieuwe adressen moeten gaan. Normaliter zal uw bladerprogramma automatisch doorgaan naar één van de opgegeven adressen.
302	Moved Temporarily	De opgevraagde informatie is tijdelijk verplaatst naar een ander adres. Verzoeken zouden voorlopig naar één van de geretourneerde adressen moeten gaan. Normaliter zal uw bladerprogramma automatisch doorgaan naar één van de opgegeven adressen.
303	See Other	De gezochte informatie is te vinden op een ander adres. Normaliter zal uw bladerprogramma automatisch doorgaan naar het opgegeven adres.
304	Not Modified	Deze melding zou de *menselijke* gebruiker niet moeten zien. Deze melding geeft aan dat, wanneer een stuk informatie *opnieuw* wordt opgevraagd om te controleren of deze inmiddels is gewijzigd, de informatie nog ongewijzigd is.
305	Use Proxy	De opgevraagde informatie kan alleen via de opgegeven proxy-server worden benaderd. Normaliter zal uw bladerprogramma deze melding afhandelen.
400	Bad Request	Het verzoek om informatie kon niet worden ingewilligd, omdat er een fout zit in de adressering van de informatie (een ongeldig adres). Corrigeer het adres en probeer het opnieuw.
401	Unauthorized	U bent niet bevoegd om de gevraagde informatie te raadplegen. U hebt hier waarschijnlijk een gebruikersnaam en wachtwoord voor nodig.
402	Payment Required	Deze melding geeft aan dat er op de een of andere wijze een elektronische betaling moet plaatsvinden voordat u de gevraagde informatie kunt raadplegen.
403	Forbidden	U mag, om al dan niet nader verklaarde redenen, de betreffende informatie niet raadplegen. Een mogelijkheid is dat u de informatie probeert te raadplegen vanaf een onbevoegde machine.
404	Not Found	U hebt geprobeerd een bepaalde webpagina of een andere informatie op te vragen, maar de webserver kon de informatie niet vinden. Mogelijk hebt u een oude verwijzing gevolgd of een verkeerd adres ingetypt.

405	Method Not Allowed	Deze melding geeft aan dat uw bladerprogramma op de verkeerde wijze een verzoek heeft ingediend om de gewenste informatie op te vragen. Mogelijk komt dit doordat er in de verwijzende pagina een fout zit.
406	Not Acceptable	De webserver is niet in staat om de opgevraagde informatie in een formaat te leveren, dat uw bladerprogramma kan verwerken.
407	Proxy Authentication Required	U dient zich eerst aan te melden bij de proxy-server voordat u de informatie kunt opvragen. Waarschijnlijk krijgt u een venster gepresenteerd, waarin u een naam en wachtwoord dient in te vullen. Deze melding zal verschijnen indien het niet lukt om aan te melden.
408	Request Timed Out	Het verzoek kon niet worden behandeld binnen de tijd die de server handhaaft als maximale wachttijd. Mogelijk is de server te zwaar belast of is een berekening die de server moet uitvoeren om de gewenste informatie te presenteren, erg complex en tijdrovend. U kunt eventueel op een later tijdstip proberen om de informatie alsnog op te vragen.
409	Conflict	Er is een probleem opgetreden bij het benaderen van de informatie op de server. Mogelijk is iemand anders net bezig om de informatie te wijzigen, waardoor de server de informatie niet kan raadplegen. Waar mogelijk zal het bericht voldoende informatie bevatten om het probleem te kunnen achterhalen, hoewel deze informatie mogelijk alleen door een deskundige te begrijpen is.
410	Gone	De opgevraagde informatie is niet langer beschikbaar en er is ook geen alternatief adres bekend.
411	Length Required	Uw bladerprogramma heeft de server niet voorzien van de vereiste informatie over de lengte van het ingediende verzoek. U zou kunnen proberen de informatie met een ander bladerprogramma of een nieuwere versie van uw huidige programma op te vragen.
412	Precondition Failed	Bij het indienen van het verzoek is extra informatie (een aantal voorwaarden) aan het verzoek toegevoegd om de server in staat te stellen om de juiste informatie te vinden. Desondanks bleek de server niet in staat om informatie te vinden, die aan alle gestelde voorwaarden voldoet.
413	Request Entity Too Large	De server weigert om de opgevraagde informatie beschikbaar te stellen, omdat deze te groot in omvang is.
414	Request-URI Too Long	Het ingediende verzoek is van een te grote lengte. Mogelijk is een fout in het opgegeven adres, met teveel extra informatie, geslopen.
415	Unsupported Media Type	De server was niet in staat om de opgevraagde informatie te verwerken en aan u te geven.

500	Internal Server Error	Er is een probleem in de server ontstaan. Waarschijnlijk is er een probleem met een deel van de instellingen of functioneert een script dat dynamisch informatie moet genereren, niet correct. Veelal wordt u bij het optreden van een dergelijke fout gevraagd om de beheerder van de webserver in te lichten.
501	Not Implemented	De server ondersteunt niet de functionaliteit die noodzakelijk is om uw verzoek in te willigen.
502	Bad Gateway	U kunt deze melding krijgen van een server die als ‘proxy’ of als ‘gateway’ optreedt, welke een foutmelding of een ongeldige reactie heeft ontvangen van de machine die de informatie werkelijk bevat.
503	Service Unavailable	De server is tijdelijk niet beschikbaar, wegens overbelasting of vanwege onderhoud. U kunt op een later tijdstip proberen de informatie alsnog op te vragen.
504	Gateway Timeout	U kunt deze melding krijgen van een server die als ‘proxy’ of als ‘gateway’ optreedt, welke niet op tijd de gevraagde informatie heeft ontvangen van de machine die de informatie werkelijk bevat.
505	HTTP Version Not Supported	Uw bladerprogramma heeft getracht met de server te communiceren in een versie van het HTTP-protocol, die (nog) niet door de server wordt ondersteund.

7.3 FTP

Nummer	Engelse melding	Nederlandse omschrijving
202	Command not implemented, superfluous at this site.	Het commando dat uw FTP-programma aan de FTP-server heeft doorgegeven, is niet geïmplementeerd op de FTP-server, omdat het een overbodig commando zou zijn.
331	User name okay, need password.	De opgegeven gebruikersnaam is geaccepteerd, maar er is nog een wachtwoord vereist.
332	Need account for login.	De opgegeven gebruikersnaam en het wachtwoord zijn geaccepteerd, maar u dient nog een ‘accountnaam’ op te geven om u te kunnen aanmelden.
421	Service not available, closing control connection.	De dienst is niet beschikbaar en de verbinding is verbroken. Dit antwoord kan op vrijwel elke opdracht worden gegeven wanneer het systeem weet dat het moet afsluiten.
425	Can’t open data connection.	Het is niet gelukt om een dataverbinding te openen. Om dit te begrijpen, is enig begrip van het FTP-protocol vereist. FTP gebruikt twee ‘kanalen’: één kanaal wordt voor de besturing gebruikt, het andere voor de overdracht van gegevens. Het tweede kanaal wordt echter pas geopend op het moment dat dit vereist is, en is niet gebonden aan een vast poortnummer. Indien op de verzendende of de ontvangende machine geen poort meer beschikbaar is, kan deze melding worden gegeven.
426	Connection closed; transfer aborted.	De verbinding is verbroken, omdat de overdracht is afgebroken

450	Requested file action not taken. File unavailable (e.g., file busy).	Het opgevraagde bestand is niet beschikbaar. Mogelijk bestaat het bestand wel, maar is het in gebruik door een ander proces op de FTP-server.
451	Requested action aborted: local error in processing.	De uitvoering van een verzoek is afgebroken, omdat er een fout is opgetreden in de verwerking van de gegevens.
452	Requested action not taken. Insufficient storage space in system.	Een verzoek is niet uitgevoerd, omdat er onvoldoende schijfruimte is op de FTP-server.
500	Syntax error, command unrecognized.	Er is een fout geconstateerd in het opgegeven commando. Dit kan duiden op een fout in uw FTP-programma, maar het kan ook betekenen dat er een te lang commando is gegeven, waar de FTP-server niet mee overweg kan.
501	Syntax error in parameters or arguments.	De parameters of aanvullende informatie bij een opgegeven commando zijn niet correct geformuleerd.
502	Command not implemented.	Uw FTP-programma heeft een commando aan de FTP-server gegeven, dat niet is geïmplementeerd op de FTP-server; waarschijnlijk betreft het een commando dat volgens de specificaties niet verplicht hoeft te worden geïmplementeerd.
503	Bad sequence of commands.	De volgorde waarin uw FTP-programma een aantal commando's heeft aangeroepen, is niet correct.
504	Command not implemented for that parameter.	Het commando dat uw FTP-programma heeft gegeven aan de webserver, kan normaliter wel worden uitgevoerd, maar is niet beschikbaar met de opgegeven parameters.
530	Not logged in.	U probeert een opdracht uit te voeren, waarvoor u zich eerst dient aan te melden. Mogelijk is het u niet opgevallen dat de aanmelding niet is geslaagd. Probeer alsnog aan te melden en opnieuw uw opdracht uit te laten voeren.
532	Need account for storing files.	Voor sommige systemen dient u, zoals in het geval dat u deze melding krijgt, een 'accountnaam' op te geven bij het aanmelden. Probeer opnieuw aan te melden op het systeem, met vermelding van de vereiste accountnaam, en probeer daarna opnieuw uw bestand op de FTP-server op te slaan.
550	Requested action not taken. File unavailable.	De gevraagde actie kon niet worden uitgevoerd, omdat het bestand waarop de actie betrekking heeft, niet beschikbaar is. Mogelijk bestaat het bestand niet of niet meer, of u hebt onvoldoende rechten om de actie op het bestand uit te voeren.
551	Requested action aborted: page type unknown.	De gevraagde actie is afgebroken. De overdracht van gegevens wordt in 'pagina's' verdeeld, waarbij voor een pagina een voor de server onbekend type is opgegeven. Waarschijnlijk zijn uw FTP-programma en de FTP-server niet compatibel.
552	Requested file action aborted. Exceeded storage allocation (for current directory or dataset).	De gevraagde actie die u wilde uitvoeren op een bepaald bestand, is afgebroken. De beschikbare opslagruimte is onvoldoende voor de huidige map of gegevensverzameling.

553	Requested action not taken. File name not allowed.	U hebt geprobeerd een bestand te verzenden naar de FTP-server of om de naam van een bestand op de FTP-server te wijzigen, maar er komen waarschijnlijk karakters in voor, die de FTP-server niet aan kan.

Handboek

Aansluiting van het schoolnetwerk op kennisnet

Deel IV: Diensten

Indeling van deel IV

Dit deel van het Handboek Kennisnet behandelt een aantal speciale diensten van kennisnet.

Hoofdstuk 8 behandelt het beheren van de gegevens van de gebruikers met de Kennisnet Gebruikersadministratie.

Hoofdstuk 9 behandelt het e-mailen met de Kennisnet Webmail.

Hoofdstuk 10 behandelt het beheren van de website van uw organisatie met het Kennisnet Webhotel.

Hoofdstuk 11 behandelt het afspelen van geluid- en filmbestanden met de Kennisnet Realserver.

In Hoofdstuk 12 worden hulpmiddelen en literatuur genoemd voor het maken van websites.

8. Kennisnet Gebruikersadministratie

In dit hoofdstuk wordt uitgelegd hoe u, als ICT-coördinator binnen uw organisatie, de gebruikersadministratie voor kennisnet bijhoudt: het beheren van de gegevens van de gebruikers van kennisnet. Met 'beheren' wordt het volgende bedoeld:

- het verzamelen van de benodigde gegevens van de gebruikers, waarbij onderscheid wordt gemaakt tussen leerlingen, docenten, systeembeheerders en andere functiegroepen;
- het aanmelden bij kennisnet van de benodigde gegevens van de gebruikers;
- het, indien nodig, wijzigen en/of verwijderen van de gegevens van de gebruikers;
- het, indien gewenst, indelen van de gebruikers in gebruikersgroepen.

De gegevens die u gaat beheren zijn noodzakelijk om de gebruikers te kunnen laten werken met e-mail en met alle diensten die op kennisnet beschikbaar zijn.

Voornaamste doel zal daarom zijn om aan iedereen een gebruikersnaam, een wachtwoord en een mailadres toe te wijzen. Zonder die identificatiemiddelen zijn de e-mail en de diensten niet te gebruiken. Het is tevens uw taak om deze identificaties aan de gebruikers bekend te maken.

8.1 Benodigdheden voor de ICT-coördinator

Als ICT-coördinator hebt u voor het bijhouden van de gebruikersadministratie het volgende nodig:

- een e-mailprogramma;
- een internet-browser (bladerprogramma voor internet);
- uw persoonlijke identificatiegegevens, zonder welke u de beheertaken niet kunt uitvoeren.

8.1.1 E-mailprogramma

E-mailprogramma's moeten worden geïnstalleerd en ingesteld. Voor het instellen beschikken E-mailprogramma's over invoervelden voor een gebruikersnaam, e-mailprotocol, mailserver en een wachtwoord. U dient deze velden in te vullen vóórdat u met de e-mail aan de slag kunt. Om toegang tot deze invoervelden te verkrijgen, moet voor elk e-mailprogramma anders worden gehandeld. Lees daarvoor de handleiding van uw e-mailprogramma. Voor enkele programma's wordt reeds uitleg gegeven in deel III.

8.1.2 Internet-browser

Internet-browsers (bladerprogramma's voor internet) moeten worden geïnstalleerd. Voor enkele browsers wordt reeds uitleg gegeven in deel III.

8.1.3 Uw persoonlijke identificatiegegevens

Om uw beheertaken te kunnen uitvoeren hebt u als ICT-coördinator de volgende identificatiegegevens nodig:

Gebruikersnaam	(bijvoorbeeld: "`jan.voorbeeld.school.plaats`")
Wachtwoord	(bijvoorbeeld: "`2FK4YA84`")
Mailadres	(bijvoorbeeld: "`jan.voorbeeld@school.plaats.kennisnet.nl`")
Subdomeinnaam school	(bijvoorbeeld: "`school.plaats`")

Deze gegevens ontvangt u nog per brief van kennisnet, of u hebt ze al ontvangen. Dat ú ze ontvangt, betekent dat u bij kennisnet geregistreerd staat als systeembeheerder voor de gebruikersadministratie van uw school.

Overigens raden we u aan om het ontvangen wachtwoord uit veiligheidsoverwegingen meteen te wijzigen in een wachtwoord dat alleen ú kent. Zie paragraaf 8.4.2.

8.2 De aanpak van de gebruikersadministratie

Allereerst dient de school beleid te maken over de gebruikersgegevens. Er moet beslist worden over al dan niet anoniem aanmelden van de gebruikers, over een systeem voor wachtwoorden (zie paragraaf 8.4), over wie de systeembeheerders worden, en zo meer. Vervolgens moet u al de benodigde gegevens verzamelen en beschikbaar hebben.

Om bij de Kennisnet Gebruikersadministratie de gegevens van de gebruikers daadwerkelijk aan te melden moet u in ieder geval altijd met de internet-browser inloggen op kennisnet. U krijgt daar de mogelijkheid om de gebruikers stuk voor stuk in te voeren. Handiger is het echter als u in staat bent om in één keer alle gebruikers tegelijk aan te melden. Ook dat doet u via kennisnet, maar dan moet u de gegevens daaraan voorafgaand in een bruikbaar bestand hebben gezet en beschikbaar hebben op uw pc of uw netwerk.

In paragraaf 8.3 leest u wat er voor zo'n bestand nodig is. U kunt die paragraaf altijd overslaan als u de gebruikers anoniem wilt aanmelden, een mogelijkheid die we niet aanraden omdat de gebruikers zich dan minder bij kennisnet betrokken zullen voelen.

8.3 Vooraf: aanmaken van een bestand met gebruikers

In deze paragraaf leest u wat u moet doen om de gegevens van de gebruikers in een bruikbaar bestand te zetten. Zo'n bestand is bedoeld als hulpmiddel om het aanmelden van gebruikers bij kennisnet te vergemakkelijken. U kunt deze paragraaf overslaan als u van plan bent om uw gebruikers stuk voor stuk bij kennisnet aan te melden. Ook als u de gebruikers anoniem wilt aanmelden, hoeft u deze paragraaf niet te lezen.

Omdat de meeste organisaties, met name scholen, wel een namenlijst van hun leerlingen en medewerkers in de computer hebben staan, is de basis voor het bestand meestal gauw gemaakt. Waar u nu nog voor moet zorgen, is dat:

- het bestand zo wordt ingedeeld dat alle benodigde gegevens erin staan;
- het bestand er op een bepaalde manier uitziet: de gegevens moeten door komma's of puntkomma's gescheiden zijn.

Voor de indeling is het makkelijk een spreadsheet-programma als Microsoft Excel of Corel Quattro te gebruiken. Dit programma moet wel over de mogelijkheid beschikken om het bestand op te slaan in zogenoemd CSV-formaat, waarover meer in paragraaf 8.3.2. Het gebruik van een spreadsheet-programma hoeft niet: u kunt ook direct een eenvoudige tekst-editor gebruiken, bijvoorbeeld Windows Kladblok (Notepad).

Let op!

Word of WordPerfect of een andere grote tekstverwerker kunt u hiervoor alleen gebruiken indien u het bestand opslaat als ASCII-tekst, DOS-tekst of iets dergelijks.

8.3.1 Indeling van het bestand

Aan de hand van een voorbeeld uit Microsoft Excel zullen we nalopen welke gegevens nodig zijn en hoe het bestand wordt ingedeeld.

Microsoft Excel - excelvoorbeeld

	A	B	C	D	E	F	G	H	I	J
1	voornaam	tussenvoegsels	achternaam	functie	gebruikersnaam	mailadres	wachtwoord	actie		
2	Alexander		Rijnbeek	systeembeheerder	alexander.rijnbeek		verandermij			
3	Denise	van	Mourik	docent	denise.van.mourik		verandermij			
4	Peter	van	Herpt	docent	peter.van.herpt		verandermij	verwijderen		
5	Roger		Boogaard	docent	roger.boogaard		verandermij	wijzigen		
6	Azzedinne		ElKaddouri	bestuurder	azzedinne.elkaddouri		verandermij			
7	Cedric		Groen	oop	cedric.groen		verandermij	aanmaken		
8	Freek	de	VriesLentsch	leerling	freek.de.vrieslentsch		verandermij			
9	Melany		Hulsbosch	leerling	melany.hulsbosch		verandermij			
10	Imran		Mohamed	leerling	imran.mohamed		verandermij			
11	Martin		Linthorst	leerling	martin.linthorst		verandermij	wijzigen		
12	Roderick		Caciano	leerling	roderick.caciano		verandermij			
13	Perez		Balsemhof	leerling	perez.balsemhof		verandermij			
14	Danny		Pistenr	leerling	danny.pistenr		verandermij			
15	Rowena		Scheepers	leerling	rowena.scheepers		verandermij			
16	Mirjam		Scholtens	leerling	mirjam.scholtens		verandermij			
17	Ben	vanden	Bruber	leerling	ben.vanden.bruber		verandermij			
18	Ruurd-Jan		Zwarts	leerling	ruurd-jan.zwarts		verandermij			
19	Tamara		Otto	leerling	tamara.otto		verandermij			
20	Mariella		Benus	leerling	mariella.benus		verandermij			
21	Frank		Hazeleger	leerling	frank.hazeleger		verandermij	verwijderen		
22	Maaike		Holzmann	leerling	maaike.holzmann		verandermij			
23	Ruth		Koger	leerling	ruth.koger		verandermij			
24	Jitse		Schraphok	leerling	jitse.schraphok		verandermij			
25										

Figuur 105: Voorbeeldbestand uit Microsoft Excel

In rij 1, de kop, van het voorbeeldbestand ziet u boven elke kolom de namen van de gegevens (‘voornaam’, ‘tussenvoegsels’, enzovoort); in de kolommen daaronder vindt u de gegevens zelf. Welke kolom bevat wat?

Dat mag u eigenlijk zelf beslissen, omdat bij het aanmelden straks de namen van de gegevens door onze software worden herkend. U kunt het bovenstaande voorbeeld dus evengoed op een andere manier indelen, als dat gemakkelijker voor u is. Bijvoorbeeld:

achternaam	voornaam	enzovoort
Rijnbeek	Alexander	enzovoort
Mourik	Denise	enzovoort

Dit betekent voor onze software precies hetzelfde als het voorbeeld van Figuur 105.

8.3.1.1 Welke gegevens moet u aanleveren?

U hebt hierbij binnen bepaalde grenzen zelf de keus:

gebruikersnaam	Wat elke gebruiker hoe dan ook nodig heeft, is een ‘gebruikersnaam’. Deze mag u zelf aanleveren (als u bijvoorbeeld al gebruikersnamen hebt op uw lokale netwerk kan dat handig zijn). Hebt u echter geen gebruikersnamen, dan kunt u ook gewoon ‘voornaam’ en ‘achternaam’ aanleveren, zoals in bovenstaande voorbeelden. Onze software maakt daar dan voor u gebruikersnamen van.
mailadres	Als uw school geen eigen mailserver heeft, dus als kennisnet uw e-mail afhandelt, dan moeten wij ook de ‘mailadressen’ van uw gebruikers weten. Hier hebt u dezelfde keuze als bij de gebruikersnamen. U kunt een kolom mailadres in uw bestand zetten waarin u zelf per gebruiker een mailadres opgeeft, of u kunt onze software mailadressen laten maken van de ‘voornaam’ en ‘achternaam’.
functie	Verder moet u per gebruiker een ‘functie’ opgeven. Hierbij kunt u kiezen uit: “docent”, “bestuurder”, “leerling”, “oop” (onderwijs-ondersteunend personeel), of “systeembeheerder”.

8.3.1.2 Welke gegevens kunt u aanleveren?

De volgende namen van gegevens worden momenteel door onze software herkend wanneer u ze als namen boven de kolommen gebruikt:

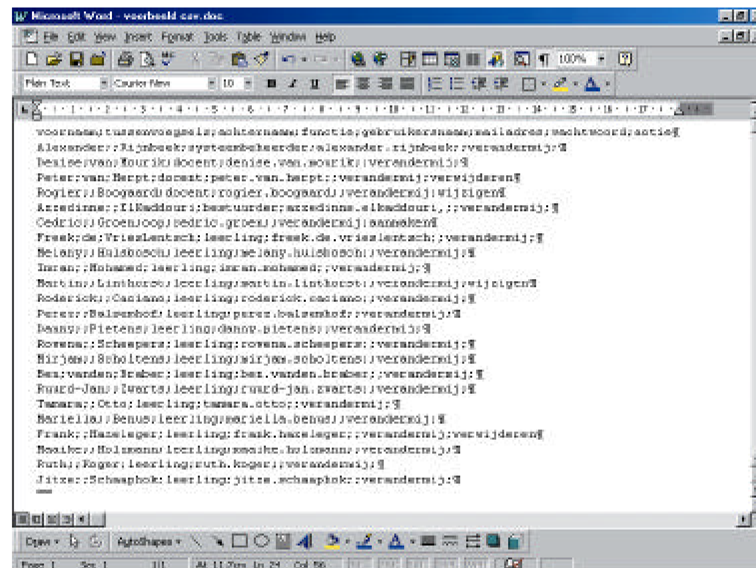
gebruikersnaam	Als u dit niet opgeeft, zijn ‘voornaam’ en/of ‘achternaam’ verplicht.

mailadres	Als u geen eigen mailserver heeft en deze kolom weglaat, dan zijn ook 'voornaam' en/of 'achternaam' nodig. Als deze ook ontbreken zal de software van kennisnet proberen van de door u aangeleverde 'gebruikersnaam' een mailadres te maken.
wachtwoord	U kunt de wachtwoorden van uw gebruikers zelf bedenken en hier opgeven. U kunt ze ook weglaten. Onze software maakt dan wachtwoorden van 8 willekeurige letters en cijfers, die u krijgt teruggemeld.
voornaam	Nodig om 'gebruikersnaam' en/of 'mailadres' te maken als u deze hebt weggelaten.
tussenvoegsels	Het kan zijn dat u het handig vindt om tussenvoegsels ("van", "van der", enzovoort) in de namen apart te vermelden. Deze worden voor de 'achternaam' gevoegd.
achternaam	Zie 'voornaam'.
functie	Kan indicatief zijn voor de rechten die de gebruiker straks op kennisnet heeft. Vul hier "docent", "bestuurder", "leerling", "oop" (onderwijs-ondersteunend personeel) of "systeembeheerder" in.
mailbox	Geeft aan hoeveel opslagruimte (in megabytes) er voor deze gebruiker maximaal op de kennisnet-mailserver beschikbaar is. Standaard is 10 MB. Denk eraan dat als uw organisatie gemiddeld meer dan 10 MB per gebruiker heeft ingesteld daarvoor extra moet worden betaald. De hier opgegeven waarden worden naar boven afgerond op tientallen megabytes.
actie	Geeft aan wat met de opgegeven gebruiker moet gebeuren. Als deze kolom wordt weggelaten of niet ingevuld, wordt "aanmaken" verondersteld. Andere mogelijke waarden zijn "wijzigen" en "verwijderen", maar die hebt u pas nodig als er al gebruikers aangemeld zijn.

8.3.2 Hoe het bestand er uitziet: kommagescheiden (CSV)

Het bestand moet er op een bepaalde manier uitzien: we spreken over het 'formaat' van het bestand. Het formaat dat nodig is voor kennisnet heet 'kommagescheiden'; dergelijke bestanden hebben meestal de extensie ".CSV" (Comma Separated Values). Kommagescheiden betekent dat elk gegeven van de andere gegevens gescheiden moet zijn door een komma of een puntkomma. De meeste spreadsheet- en database-programma's kunnen CSV-bestanden aanmaken met de optie 'Opslaan als' en als bestandstype "CSV". Microsoft Excel of Corel Quattro zullen uw spreadsheet als CSV-bestand dan ook opslaan door elke rij van uw werkblad op een regel te zetten, en de kolommen per regel met (punt)komma's te scheiden.

Eigenlijk ziet een CSV-bestand voor kennisnet er dus heel simpel uit. Elke gebruiker staat op een regel, en de gegevens van de gebruiker worden gescheiden door komma's of puntkomma's zoals in de CSV-versie van onze voorbeeldbestand uit Microsoft Excel.



Figuur 106: CSV-versie van voorbeeldbestand

U begrijpt nu ook dat u de gegevens zelf makkelijk met een eenvoudige tekst-editor in CSV-formaat kunt zetten. Let er alleen op dat ook ontbrekende gegevens een (punt)komma nodig hebben, zoals u in Figuur 106 ziet bij de ontbrekende 'ma iladressen'.

Samenvattend: hoe u het bestand voor de Kennisnet Gebruikersadministratie ook aanmaakt, u kunt het op kennisnet alleen gebruiken in CSV-formaat, en níet in het oorspronkelijke formaat van bijvoorbeeld Excel of Quattro.

8.4 Wachtwoorden

8.4.1 Bedenken en onthouden van wachtwoorden

Wachtwoorden zijn persoonlijk en geven toegang tot persoonlijke gegevens. Het is daarom niet wenselijk dat een gebruikersnaam met wachtwoord gebruikt kan worden door een andere gebruiker. Als wachtwoorden makkelijk te raden of te achterhalen zijn, dan bestaat het gevaar dat personen zich op kennisnet kunnen voordoen als iemand anders. Hierdoor wordt het onmogelijk om onrechtmatig gebruik van kennisnet op te sporen. Organisaties als scholen moeten rekening houden met deze problematiek bij het opstellen van richtlijnen voor wachtwoordgebruik binnen de school.

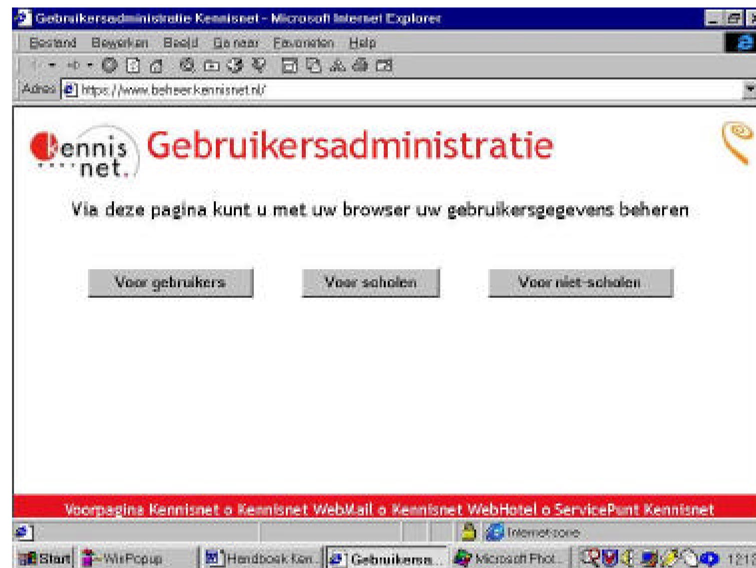
Moeilijk te kraken wachtwoorden bevatten geen bestaande woorden en zijn een combinatie van cijfers en letters met een lengte van ten minste acht tekens. Om dergelijke wachtwoorden makkelijk te onthouden, kan gebruik worden gemaakt van een bekende zin. Bijvoorbeeld: "Heb je wel gehoord van de zevensprong" wordt "Hjwgvd7s".

8.4.2 Wachtwoorden wijzigen

Omdat de beveiliging van kennisnet belangrijk is, geven we nu meteen aan hoe alle gebruikers (zowel u als systeembeheerder als andere functiegroepen) hun eígen wachtwoord voor kennisnet kunnen wijzigen.

- Start de internet-browser.
- Ga naar het adres http://www.beheer.kennisnet.nl/.

De volgende web-pagina verschijnt.



Figuur 107: Gebruikersadministratie: Gebruikersgegevens beheren

- Klik op de knop 'Voor gebruikers'.

In de webpagina die verschijnt, ziet u het volgende venster.

Wat wilt u doen?

Wachtwoord wijzigen

Alias maken

Figuur 108: Gebruikersadministratie: Wat wilt u doen?

- Klik op de knop 'Wachtwoord wijzigen'.

In de web-pagina die verschijnt, ziet u het volgende venster.

Wachtwoord wijzigen

Nieuw wachtwoord:

Nieuw wachtwoord: *(nogmaals, ter controle)*

Ga door

Figuur 109: Gebruikersadministratie: Wachtwoord wijzigen

- Voer twee keer het nieuwe wachtwoord in.
- Klik op de knop 'Ga door'.

8.4.3 Wachtwoord vergeten?

Als een gebruiker het wachtwoord vergeten is, dan kunt u – als ICT-coördinator – aan deze gebruiker een nieuw wachtwoord toekennen. Voor het invoeren van een nieuw wachtwoord gaat u met de internet-browser naar de Kennisnet Gebruikersadministratie, waar u de optie ‘GEBRUIKER Wijzig’ kiest. Hoe u inlogt op de gebruikersadministratie, leest u in paragraaf 8.6. Over de optie leest u meer in paragraaf 8.10. Natuurlijk moet die gebruiker al wel zijn aangemeld.

8.5 Meerdere vestigingen beheren

Op de web-pagina’s die in de volgende paragrafen aan de orde komen, kunt u steeds alleen de vestiging beheren waarvoor u met de toepasselijke gebruikersnaam op de beheer-website van kennisnet bent ingelogd. U mag echter in het veld ‘Gebruikersnaam’ of ‘Uw gebruikersnaam’, dat op alle web-pagina’s voorkomt, de gebruikersnaam invoeren voor een andere vestiging waarover u het beheer voert. Zo kunt u steeds omschakelen tijdens uw beheertaken, waarbij u wel altijd opnieuw het bijbehorende wachtwoord moet invoeren.

8.6 Op de Kennisnet Gebruikersadministratie inloggen

Voor het uitvoeren van de beheertaken moet u inloggen op de Kennisnet Gebruikersadministratie:

- Start de internet-browser.
- Ga naar het adres http://www.beheer.kennisnet.nl/.

De web-pagina van Figuur 107 verschijnt:

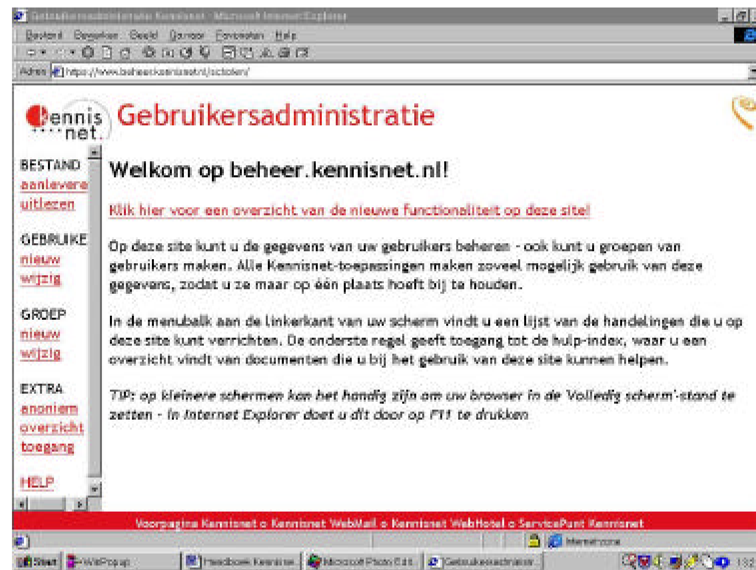
- Klik op de knop ‘Voor scholen’.

In de web-pagina verschijnt het volgende venster.

Figuur 110: Gebruikersadministratie: Netwerkwachtwoord opgeven

- Voer in het veld ‘Gebruikersnaam’ uw gebruikersnaam in.
- Voer in het veld ‘Wachtwoord’ uw wachtwoord in.
- Klik op de knop ‘OK’.

De volgende web-pagina verschijnt.



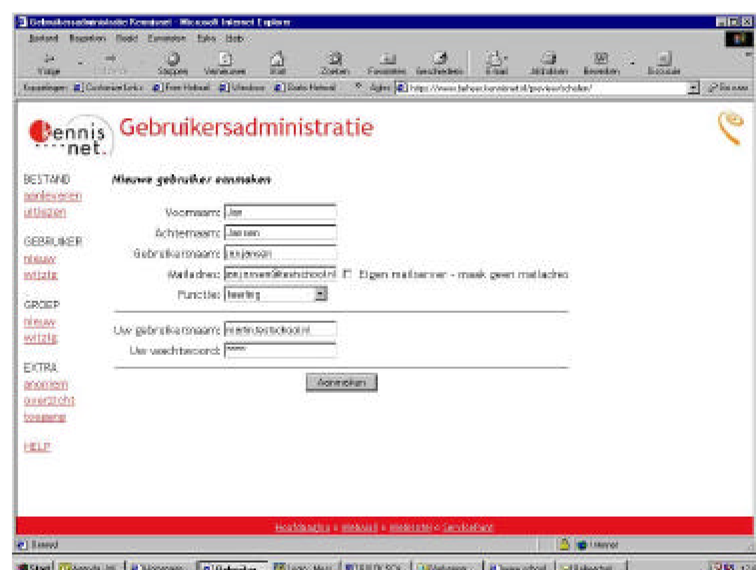
Figuur 111: Gebruikersadministratie: Welkom op beheer.kennisnet.nl!

8.7 Gebruikers aanmelden

Om gebruikers bij de gebruikersadministratie aan te melden doet u in de web-pagina van Figuur 111 het volgende:

- Klik in de linker menubalk op de optie ‘GEBRUIKER nieuw’.

De volgende web-pagina verschijnt.



Figuur 112: Gebruikersadministratie: Nieuwe gebruiker aanmaken

Op deze web-pagina kunt u nieuwe gebruikers één voor één bij kennisnet aanmelden. In de linker menubalk van de web-pagina kunt u ook andere mogelijkheden kiezen, waaronder ‘BESTAND aanleveren’ waarmee u de gebruikers aanmeldt met een CSV-bestand, zie paragraaf 8.7.2.

In het veld 'Uw gebruikersnaam' staat de gebruikersnaam al ingevuld waarmee u bij de website bent ingelogd. U kunt de gebruikersnaam nog wel veranderen (als u bijvoorbeeld de gebruikersnamen van een andere vestiging wilt aanmaken, hoeft u niet uw internet-browser te sluiten en opnieuw te beginnen), maar meestal is dat niet nodig.

8.7.1 Gebruikers een voor een aanmelden

Om de gebruikers een voor een aan te melden doet u in de web-pagina van Figuur 112 voor elke nieuwe gebruiker het volgende:

- Voer in het veld 'Uw wachtwoord' het wachtwoord in dat hoort bij de ingevulde gebruikersnaam in het veld 'Uw gebruikersnaam'.
- Voer in het veld 'Voornaam' de voornaam van de nieuwe gebruiker in.
- Voer in het 'Achternaam' de achternaam van de nieuwe gebruiker in.
- Voer, als u de gebruikersnaam zelf wilt bepalen, in het veld 'Gebruikersnaam' de gebruikersnaam van de nieuwe gebruiker in. Als u dit veld leeg laat, bepaalt de software de gebruikersnaam.
- Voer, als u het mailadres zelf wilt bepalen, in het veld 'Mailadres' het mailadres van de nieuwe gebruiker in. Als u dit veld leeg laat, bepaalt de software het mailadres.
- Als u niet wilt dat kennisnet de mailadressen aanmaakt: selecteer het aanvinkvakje 'Eigen mailserver - maak geen mailadressen'. U kunt dan de mailadressen van uw eigen mailserver blijven gebruiken.

Controleer nu of u alle velden juist hebt ingevoerd en de juiste aanvinkvakjes hebt geselecteerd. Vervolgens doet u:

- Klik op de knop 'Aanmaken'.

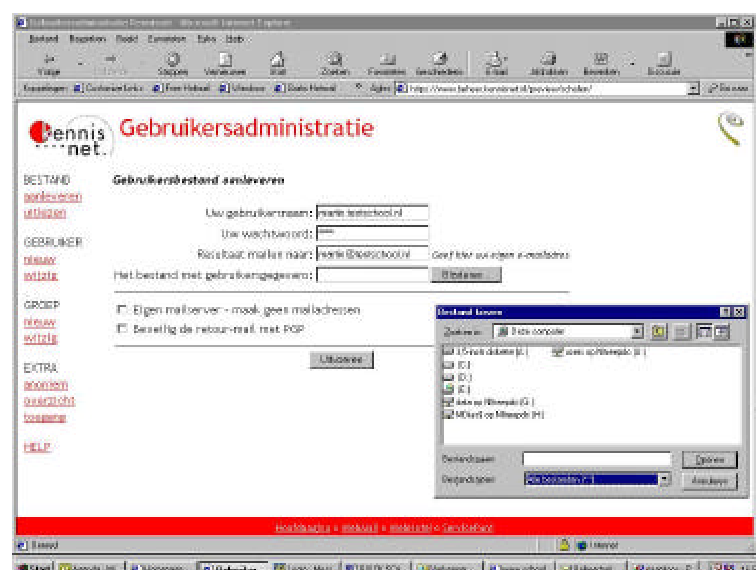
U krijgt altijd bericht terug over de gebruikers die u hebt aangemeld. Lees aan het eind van paragraaf 8.7.2 welke stappen er dan nog volgen.

8.7.2 Gebruikers met CSV-bestand aanmelden

Om de gebruikers met een CSV-bestand aan te melden doet u in de web-pagina van Figuur 112 het volgende:

- Klik in de linker menubalk op de optie 'BESTAND aanleveren'.

De volgende web-pagina verschijnt.



Figuur 113: Gebruikersadministratie: Gebruikersbestand aanleveren

- Voer in het veld 'Uw wachtwoord' het wachtwoord in dat hoort bij de ingevulde gebruikersnaam in het veld 'Uw gebruikersnaam'.
- Voer in het veld 'Resultaat mailen naar' uw eigen mailadres in. U ontvangt namelijk als resultaat een CSV-bestand terug waarin onze software uw gegevens heeft aangevuld. Of u krijgt een bericht over geconstateerde fouten.
- Als u niet wilt dat kennisnet de mailadressen aanmaakt: selecteer het aanvinkvakje 'Eigen mailserver - maak geen mailadressen'. U kunt dan de mailadressen van uw eigen mailserver blijven gebruiken.
- Als u met het beveiligingsprogramma PGP (Pretty Good Privacy) of GnuPG (GNU Privacy Guard) werkt: selecteer het aanvinkvakje 'Beveilig de retour-mail met PGP'. Uw bestand met aanvullingen wordt dan teruggestuurd in gecodeerde vorm. U kunt het in PGP of GnuPG met behulp van uw kennisnet-wachtwoord weer ontcijferen.
- Voer in het veld 'Het bestand met gebruikersgegevens' de naam, inclusief het hele pad, van het CSV-bestand in dat u hebt aangemaakt en dat u beschikbaar hebt op uw pc of uw netwerk. Makkelijker is het om te klikken op de knop 'Bladeren'. Met het venster dat dan verschijnt, kunt u het CSV-bestand opzoeken en aanklikken. De naam en het pad van het bestand verschijnen in het veld 'Het bestand met gebruikersgegevens'.

Controleer nu of u alle velden juist hebt ingevoerd en de juiste aanvinkvakjes hebt geselecteerd. Vervolgens doet u:

- Klik op de knop 'Uitvoeren'.

Nu wordt uw bestand opgestuurd naar kennisnet. U krijgt een korte mededeling te zien die u vertelt dat u nog een e-mail ontvangt met de resultaten van de verwerking.

Normaal gesproken ontvangt u binnen enkele minuten op uw mailadres antwoord. Het kan zijn dat uw CSV-bestand niet of slechts gedeeltelijk kon worden verwerkt. In dat geval heeft de e-mail die u terugkrijgt een aanhangsel waarin de fouten worden opgesomd die onze software is tegengekomen.

Meestal zal het echter zo zijn dat onze software voor u de gegevens heeft aangevuld. Hebt u bijvoorbeeld een bestand aangeleverd met de namen van uw leerlingen erin, als volgt:

```
voornaam,tussenvoegsels,achternaam
Jan,,Jansen
Piet,de,Visser
enzovoort
```

Dan krijgt u via de e-mail een bestand terug waarin allerlei nieuwe kolommen voor u zijn ingevuld. Dat zou er zo uit kunnen zien:

```
actie,gebruikersnaam,mailadres,wachtwoord,voornaam,tussenvoegsels,achternaam,functie,mailbox,
aanmaken,jan.jansen.voorbeeldschool.nl,jan.jansen@voorbeeldschool.nl,9adDsA00,Jan,,Jansen,onbekend,10
aanmaken,piet.devisser.voorbeeldschool.nl,piet.devisser@voorbeeldschool.nl,4Va88dFX,Piet,,de Vries,onbekend,10
enzovoort
```

Let op!

Er zijn nu nog geen gegevens bij kennisnet aangemeld. U ontvangt het bestand namelijk eerst terug om te bekijken of de aanvullingen correct zijn.

Controleer dan ook goed of de aanvullingen correct zijn. Bewaar tevens dit terugontvangen bestand!

Als u tevreden bent met het aangevulde bestand dat u had teruggekregen, kunt u het opnieuw, via dezelfde web-pagina, aanleveren. Dan wordt het definitief verwerkt.

Als u een bestand had aangeleverd met alle kolommen ingevuld en dat was correct, dan wordt het bestand wel meteen de eerste keer definitief verwerkt. Ook hiervan ontvangt u per e-mail een bevestiging. Bij deze bevestiging zit dan geen CSV-bestand omdat uw bestand al correct was.

U kunt het correcte bestand bewaren en gebruiken als basis voor wijzigingen of verwijderingen die u in de toekomst eventueel wilt doorvoeren. Indien gewenst kunt u het bestand weer in een spreadsheet-programma inlezen om het daarmee te onderhouden.

Zoals u ziet, staan de wachtwoorden voor de nieuwe gebruikers erin. Het is aan te raden deze aan de gebruikers uit te delen en ze aan te sporen om de wachtwoorden uit veiligheidsoverwegingen te wijzigen. Dit kunnen gebruikers zelf doen, zie paragraaf 8.4.2.

8.8 Overzicht van de gebruikers

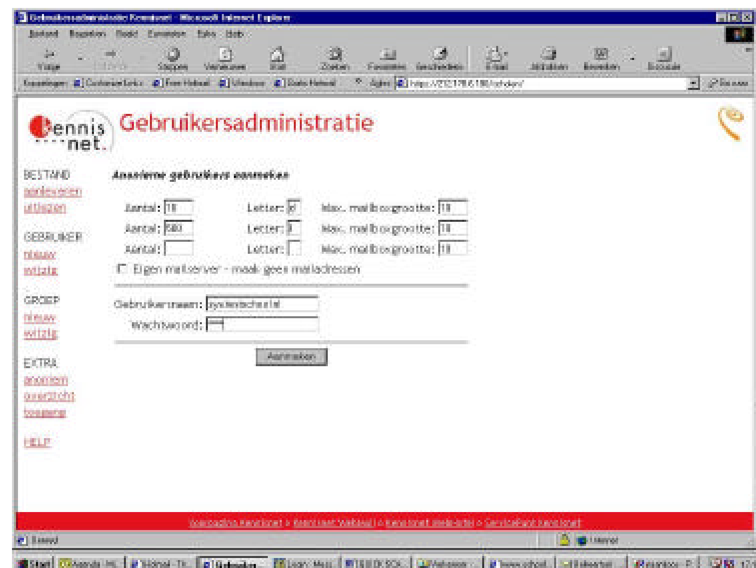
Na ontvangst van de definitieve bevestiging kunt u in een van de web-pagina's (bijvoorbeeld die van Figuur 112) met de optie 'EXTRA overzicht' aan de hand van het overzicht zien dat de gegevens zijn verwerkt. U kunt dit overzicht voortaan altijd raadplegen. Door het klikken op individuele gebruikers kunt u hun gegevens wijzigen of verwijderen.

8.9 Gebruikers anoniem aanmelden

Het kan zijn dat u de gebruikers anoniem wilt aanmelden. U kunt dan geen CSV-bestand gebruiken. In een van de web-pagina's (bijvoorbeeld die van Figuur 112) doet u het volgende:

- Klik in de linker menubalk op de optie 'EXTRA anoniem'.

De volgende web-pagina verschijnt.



Figuur 114: Gebruikersadministratie: Anonieme gebruikers aanmaken

Een anonieme gebruikersnaam ziet er als volgt uit: BRIN-nummer van uw school, gevolgd door een letter waaraan te zien is wat de functie is van de gebruiker. Namelijk: "l" voor leerling, "d" voor docent, "b" voor bestuurder, "o" voor onderwijsondersteunend personeel of "s" voor systeembeheerder. Gevolgd door een vijfcijferig volgnummer. Bijvoorbeeld: 02UCd87654.

U gaat als volgt te werk:

- Voer in het veld 'Wachtwoord' het wachtwoord in dat hoort bij de ingevulde gebruikersnaam in het veld 'Gebruikersnaam'.
- Als u niet wilt dat kennisnet de mailadressen aanmaakt: selecteer het aanvinkvakje 'Eigen mailserver - maak geen mailadressen'. U kunt dan de mailadressen van uw eigen mailserver blijven gebruiken.

- Voer in de velden 'Aantal', 'Letter' en 'Max. mailboxgrootte' de aantallen en functietypes ("l" voor leerling, "d" voor docent, "b" voor bestuurder, "o" voor oop, "s" voor systeembeheerder) en groottes in van de mailadressen die u nodig hebt. Voor meer dan 10 MB aan mailboxgrootte moet extra worden betaald.

Controleer nu of u alle velden juist hebt ingevoerd en de juiste aanvinkvakjes hebt geselecteerd. Vervolgens doet u:

- Klik op de knop 'Aanmaken'.

De mailadressen worden vervolgens door onze software voor u aangemaakt met oplopende cijferreeksen en aan u teruggemeld.

Let op!

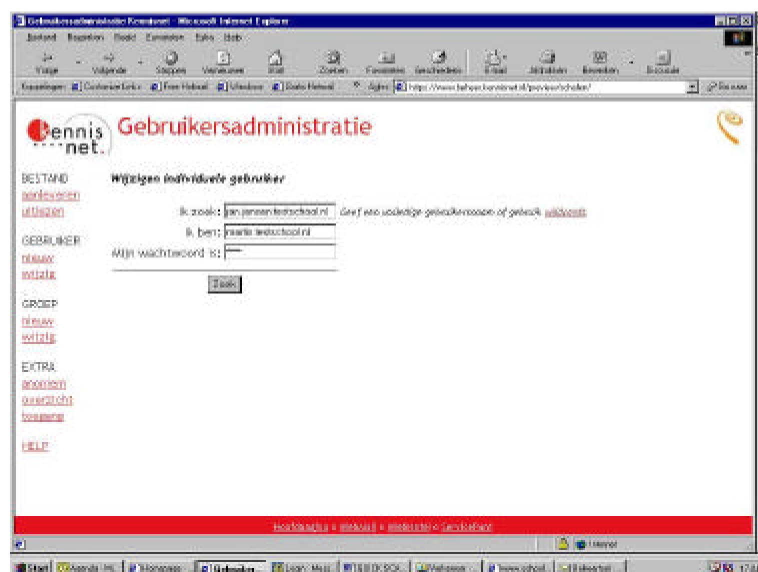
Zodra u klikt op 'Aanmaken', zal het systeem met het aanmaken beginnen. Het resultaat daarvan – de wachtwoorden en mailadressen – krijgt u direct teruggemeld. U dient deze lijst af te drukken en te bewaren, de gegevens worden namelijk niet opgeslagen. De afdruk kunt u gebruiken om de adressen en wachtwoorden aan uw gebruikers toe te wijzen.

8.10 Individuele gebruikers wijzigen

Het kan zijn dat u de gegevens van individuele gebruikers wilt wijzigen. U zou een CSV-bestand kunnen gebruiken met als actie voor de betrokken gebruikers "Wijzigen". Als het om enkele gebruikers gaat, kunt u sneller in een van de web-pagina's (bijvoorbeeld die van Figuur 112) het volgende doen:

- Klik in de linker menubalk op de optie 'GEBRUIKER wijzig'.

De volgende web-pagina verschijnt.



Figuur 115: Gebruikersadministratie: Wijzigen individuele gebruiker

U gaat als volgt te werk:

- Voer in het veld 'Mijn wachtwoord is' het wachtwoord in dat hoort bij de gebruikersnaam die op de website is ingelogd en die staat in het veld 'Ik ben'.
- Voer in het veld 'Ik zoek' de gebruikersnaam van de gebruiker die u zoekt in.

Controleer nu of u alle velden juist hebt ingevoerd en de juiste aanvinkvakjes hebt geselecteerd. Vervolgens doet u:

- Klik op de knop 'Zoek'.

U kunt nu de gegevens wijzigen.

8.11 Gebruikersgroepen aanmaken

Voor meerdere kennisnet-toepassingen (bijvoorbeeld het Kennisnet Webhotel, zie hoofdstuk 10) kan het handig zijn om uw gebruikers in groepen in te delen. Een belangrijke toepassing van groepen is dat u ze als mailinglijsten kunt gebruiken. Als u een groep namelijk een mailadres geeft, en naar dat adres wordt een e-mail gestuurd, dan zal de kennisnet-mailserver het mailtje doorsturen aan alle groepsleden met een eigen mailadres.

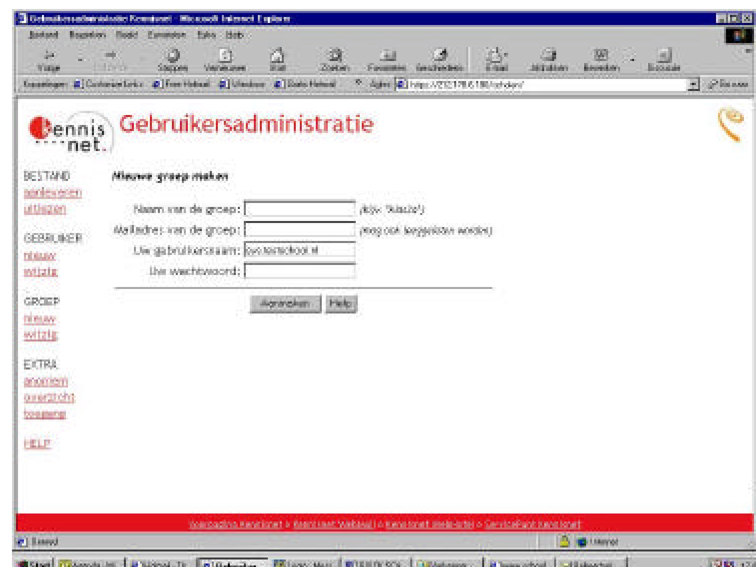
Let op!

Deze functionaliteit werkt alleen als u de kennisnet-mailserver gebruikt. Als uw school een eigen mailserver heeft, kunt u dáármee mailinglijsten maken. Zie in dat geval de handleiding van uw mailserver-software.

Om een nieuwe groep te maken doet u in een van de web-pagina's (bijvoorbeeld die van Figuur 112) het volgende:

- Klik in de linker menubalk op de optie 'GROEP nieuw'.

De volgende web-pagina verschijnt.



Figuur 116: Gebruikersadministratie: Nieuwe groep maken

U gaat als volgt te werk:

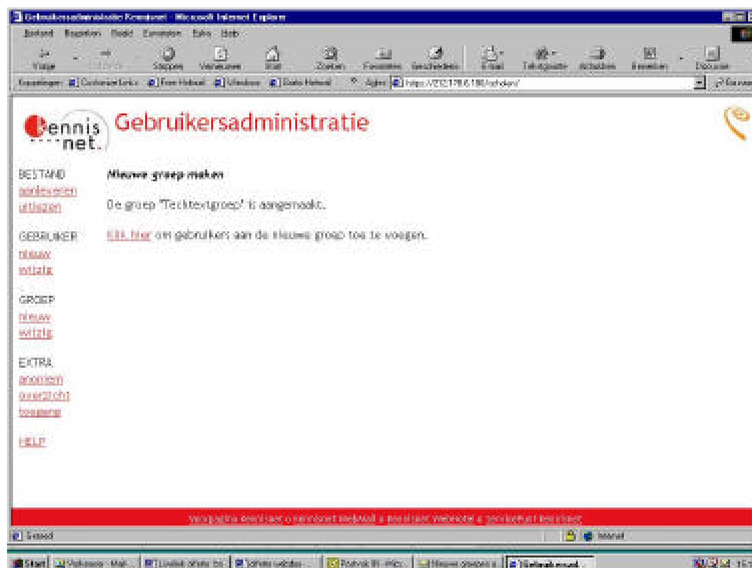
- Voer in het veld 'Uw wachtwoord' het wachtwoord in dat hoort bij de ingevulde gebruikersnaam in het veld 'Uw gebruikersnaam'.
- Voer in het veld 'Naam van de groep' een betekenisvolle naam voor de nieuwe groep in, bijvoorbeeld "Klas2a".
- Voer in het veld 'Mailadres van de groep' het mailadres in, bijvoorbeeld "klas2a@uwschool.nl". U mag het ook leeg laten, dan wordt het mailadres voor u aangemaakt.

Controleer nu of u alle velden juist hebt ingevoerd. Vervolgens doet u:

- Klik op de knop 'Aanmaken'.

Nu wordt een nieuwe groep aangemaakt met het opgegeven mailadres en uzelf als enig lid.

De volgende web-pagina verschijnt.

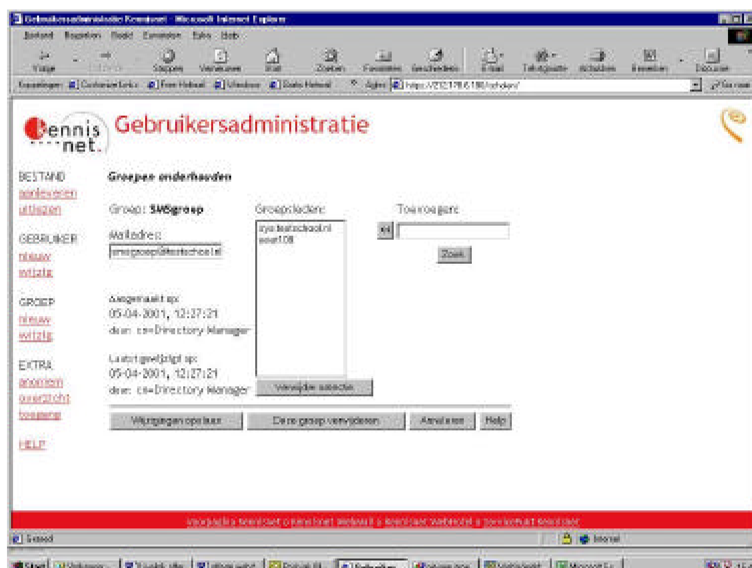


Figuur 117: Gebruikersadministratie: Nieuwe groep maken, groep is aangemaakt

- Klik op de knop ‘Klik hier’.

De web-pagina van Figuur 118 in paragraaf 8.12 verschijnt, waar u onder andere gebruikers aan de groep kunt toevoegen. Ook het verwijderen van gebruikers uit een groep, en het wijzigen van het mailadres of het verwijderen van de hele groep doet u in die web-pagina.

8.12 Gebruikers aan een groep toevoegen



Figuur 118: Gebruikersadministratie: Groepen onderhouden

In het midden van de web-pagina ziet u een blok onder ‘Groepsleden:’ met daarin de gebruikers die reeds lid zijn van de groep. Daarnaast ziet u een tekstveld, onder ‘Toevoegen:’.

Voor het toevoegen van grote aantallen gebruikers raadpleegt u paragraaf 8.12.2. Voor het toevoegen van enkele gebruikers paragraaf 8.12.1.

8.12.1 Enkele gebruikers toevoegen

- Voer in het tekstveld onder 'Toevoegen:' een gebruikersnaam in. (In plaats van een gebruikersnaam kunt u ook een mailadres invullen. Onze software zoekt daar automatisch de juiste gebruikersnaam voor u bij.)
- Klik op de 'dubbele punthaken' links van het tekstveld. De gebruikersnaam wordt toegevoegd aan de lijst met groepsleden.
- Herhaal de twee vorige stappen zo vaak u wilt.
- Verwijder eventueel weer groepsleden door onder 'Groepsleden:' een selectie te maken (hoe dat moet, hangt af van uw internet-browser, maar experimenteert u eens door te klikken met de muis in combinatie met de toetsen Ctrl, Shift of Alt). Klik daarna op de knop 'Verwijder selectie'.

Mocht u bij nader inzien toch uw toevoegingen en/of wijzigingen niet willen doorvoeren dan kunt u de pagina gewoon verlaten zonder op te slaan. U kunt ook altijd terug naar de laatst opgeslagen toestand door op de knop 'Annuleren' te klikken.

Als u wel wilt opslaan: controleer of u alle gebruikers juist hebt ingevoerd. Vervolgens doet u:

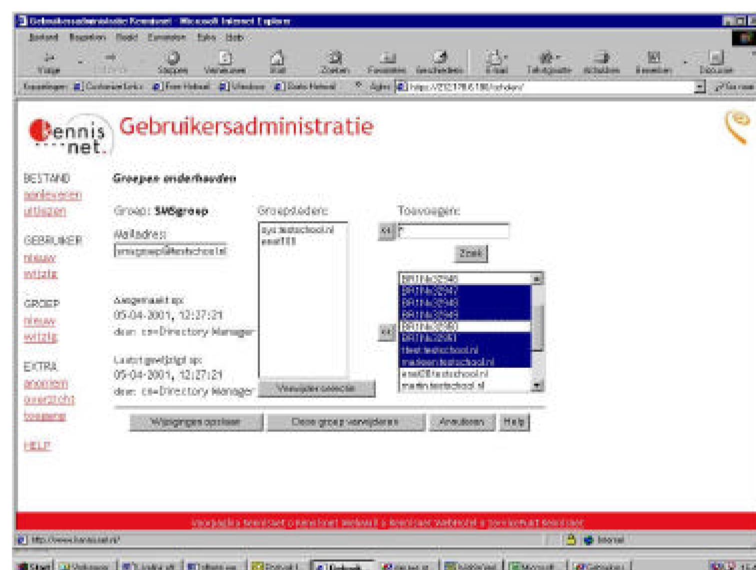
- Klik op de knop 'Wijzigingen opslaan', waarna uw veranderingen worden doorgevoerd.

8.12.2 Grote aantallen gebruikers aan een groep toevoegen

Het kan voorkomen dat u grote gebruikersgroepen wilt maken, waarvoor het wat veel werk is om alle leden één voor één in te voeren. Hiervoor gaat u als volgt te werk:

- Voer in het tekstveld onder 'Toevoegen:' een tekenreeks om mee te zoeken in, met een joker (bijvoorbeeld "n*" voor alle gebruikers die beginnen met een "n", of "fre*" voor alle gebruikers die beginnen met "fre").
- Klik op de knop 'Zoek', dan verschijnt onder deze knop een blok met al de gebruikers die voldoen aan uw zoekopdracht.

De web-pagina ziet er dan zo uit.



Figuur 119: Gebruikersadministratie: Groepen onderhouden, groot aantal gebruikers toevoegen

- Selecteer in het blok de namen die u wenst. Hoe dat moet, hangt af van uw internet-browser. Experimenteert u eens door te klikken met de muis in combinatie met de toetsen Ctrl, Shift of Alt.
- Klik op de 'dubbele punthaken' links van het blok met namen. De geselecteerde gebruikersnamen worden toegevoegd aan de lijst met groepsleden.

- Herhaal de vier vorige stappen zo vaak u wilt.
- Verwijder eventueel weer groepsleden door onder ‘Groepsleden:’ een selectie te maken (hoe dat moet, hangt af van uw internet-browser, maar experimenteert u eens door te klikken met de muis in combinatie met de toetsen Ctrl, Shift of Alt). Klik daarna op de knop ‘Verwijder selectie’.

Mocht u bij nader inzien toch uw toevoegingen en/of wijzigingen niet willen doorvoeren dan kunt u de pagina gewoon verlaten zonder op te slaan. U kunt ook altijd terug naar de laatst opgeslagen toestand door op de knop ‘Annuleren’ te klikken.

Als u wel wilt opslaan: controleer of u alle gebruikers juist hebt ingevoerd. Vervolgens doet u:

- Klik op de knop ‘Wijzigingen opslaan’, waarna uw veranderingen worden doorgevoerd.

8.13 Gebruikers uit een groep verwijderen

U kunt in de web-pagina ‘Groepen onderhouden’ (zie Figuur 118) gebruikers uit een gebruikersgroep verwijderen. U gaat als volgt te werk:

- Maak onder ‘Groepsleden:’ een selectie (hoe dat moet, hangt af van uw internet-browser, maar experimenteert u eens door te klikken met de muis in combinatie met de toetsen Ctrl, Shift of Alt).
- Klik daarna op de knop ‘Verwijder selectie’.

Mocht u bij nader inzien toch uw verwijderingen niet willen doorvoeren dan kunt u de pagina gewoon verlaten zonder op te slaan. U kunt ook altijd terug naar de laatst opgeslagen toestand door op ‘Annuleren’ te klikken.

Als u wel wilt opslaan: controleer of u alle gebruikers juist hebt verwijderd. Vervolgens doet u:

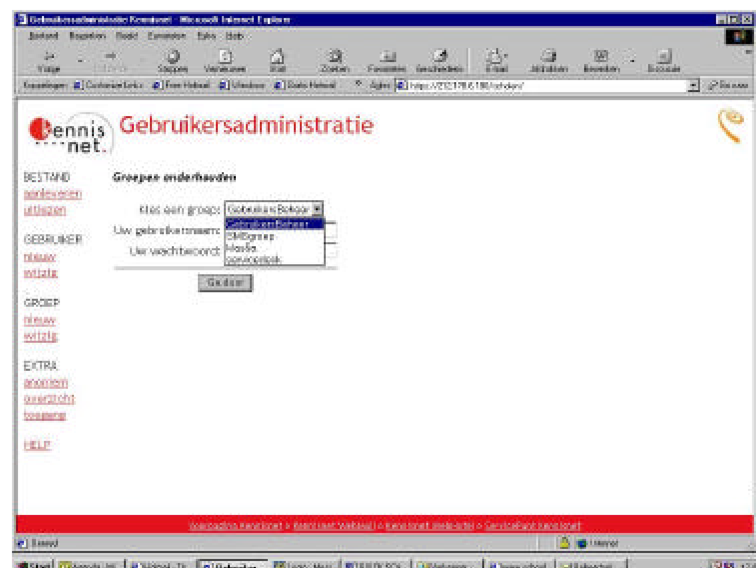
- Klik op de knop ‘Wijzigingen opslaan’, waarna uw verwijderingen worden doorgevoerd.

8.14 Gebruikersgroepen onderhouden

Om een gebruikersgroep te onderhouden (bijvoorbeeld wijzigen van gebruikers of het mailadres of helemaal verwijderen) doet u in een van de web-pagina’s (bijvoorbeeld die van Figuur 112) het volgende:

- Klik in de linker menubalk op de optie ‘GROEP wijzig’.

De volgende web-pagina verschijnt.



Figuur 120: Gebruikersadministratie: Groepen onderhouden

U gaat als volgt te werk:

- Voer in het veld 'Uw wachtwoord' het wachtwoord in dat hoort bij de ingevulde gebruikersnaam in het veld 'Uw gebruikersnaam'.
- Voer in het veld 'Kies een groep' de naam van de groep in. Klik daarvoor op het pijltje van de keuzelijst.

Controleer nu of u alle velden juist hebt ingevoerd. Vervolgens doet u:

- Klik op de knop 'Ga door'.

Hierna wordt u doorverwezen naar de web-pagina waarop u gebruikersgroepen kunt wijzigen of verwijderen. Zie Figuur 118.

U gaat als volgt te werk:

Voor gebruikers onderhouden: raadpleeg paragraaf 8.12.1.

Voor het mailadres wijzigen:

- Wijzig in het veld 'Mailadres:' het mailadres.
- Klik op de knop 'Wijzigingen opslaan'.

Voor de hele gebruikersgroep verwijderen:

- Klik op de knop 'Deze groep verwijderen'.

8.15 Systeembeheerders met wijzigingsbevoegdheid aanmelden

Sommige gebruikers hebt u aangemeld met het kenmerk "s" voor systeembeheerder. Deze gebruikers kunnen dan nog geen gegevens van andere gebruikers wijzigen. Als u ze deze bevoegdheid wilt geven, dient u ze in de web-pagina van Figuur 116 onder te brengen in de groep 'GebruikersBeheer'.

9. Kennisnet Webmail

Kennisnet biedt met Kennisnet Webmail de mogelijkheid om e-mail te lezen via het World Wide Web (internet). Dit betekent dat kennisnetgebruikers overal en altijd met een internetverbinding hun persoonlijke e-mail kunnen lezen. Ook op vakantie of op studiereis kan de gebruiker in elk internetcafé zijn e-mail ophalen en zelf e-mail versturen. Dit komt omdat de e-mail nu toegankelijk is met een internet-browser zoals Netscape Navigator of Microsoft Internet Explorer (zie deel III). De gebruiker hoeft geen instellingen te wijzigen in het e-mailprogramma dat normaal in gebruik is op de eigen pc of het werkstation. Natuurlijk blijft ook op de eigen pc of werkstation, op school of thuis, de e-mail nog te lezen.

Kennisnet Webmail biedt een scala aan mogelijkheden om op school, thuis, en op het vakantie-adres berichten uit te wisselen met contactpersonen binnen kennisnet en op internet. De gebruikers kunnen met Kennisnet Webmail direct aan de slag: ze hoeven niets aan te vragen, ook hoeven ze zich niet vooraf aan te melden. Als gebruikers eenmaal 'bekend' zijn binnen de Kennisnet Gebruikersadministratie (zie hoofdstuk 8) loggen zij eenvoudigweg met hun gebruikersnaam en wachtwoord in op Kennisnet Webmail.

Het blijft natuurlijk ook elders altijd mogelijk om andere e-mailprogramma's, zoals Microsoft Outlook, te gebruiken. Hoe u die instelt voor uw eigen situatie, kunt u vinden in deel III.

9.1 Op Kennisnet Webmail inloggen

Voor het overal ter wereld e-mailen moet u inloggen op Kennisnet Webmail:

- Start de internet-browser.
- Ga naar het adres http://webmail.kennisnet.nl/.

Op de web-pagina verschijnt het volgende venster.

Figuur 121: Kennisnet Webmail aanmelden

- Voer in het veld 'Gebruikersnaam' de gebruikersnaam in die van de ICT-coördinator (of systeembeheerder) verkregen is.
- Voer in het veld 'Wachtwoord' het wachtwoord in dat van de ICT-coördinator (of systeembeheerder) verkregen is.
- Klik op de knop 'Login'.

Daarna komt de gebruiker bij het eigen mailadres, dat van de ICT-coördinator (of systeembeheerder) verkregen is.

9.2 Uitgebreide e-mailfunctionaliteit

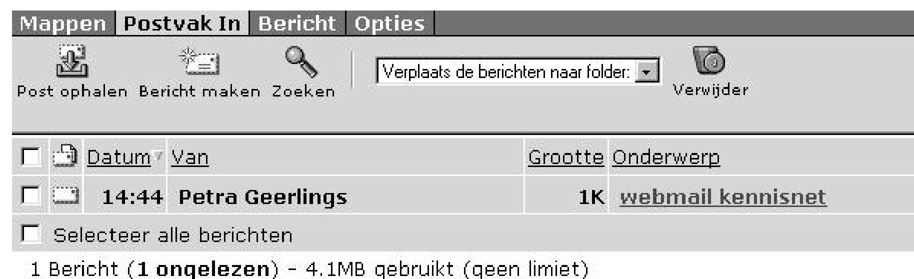
Met Kennisnet Webmail kan de gebruiker op eenvoudige wijze e-mail versturen, doorsturen, ontvangen en verwijderen uit zijn eigen mailadres op kennisnet. Daarnaast biedt webmail de mogelijkheid om e-mail te archiveren in zelf aan te maken mappen of folders. De e-mail blijft binnen het eigen mailadres beschikbaar totdat de gebruiker besluit deze op te ruimen. De ruimte in het mailadres is beperkt tot 10 MB.

9.2.1 Binnengekomen berichten bekijken

In het 'Postvak In' ziet de gebruiker de binnengekomen berichten met datum en tijd van ontvangst, afzender, grootte en onderwerp:

- Klik op de knop 'Postvak In'.

Het volgende venster verschijnt.



Figuur 122: Webmail: Postvak in

- Klik onder 'Onderwerp' op het onderwerp van het bericht om het bericht te openen en te lezen.

9.2.2 Berichten archiveren

Na het lezen van het bericht kan de gebruiker het bericht markeren voor verwijdering, of voor opbergen in een van de door hem/haar zelf aan te leggen mappen of folders.

- Klik op de knop 'Mappen' (zie Figuur 122).

Er verschijnt bijvoorbeeld:



Figuur 123: Webmail: Mappen

9.2.3 Gearchiveerde berichten: trefwoorden zoeken

De gebruiker kan zoeken in de opgeborgen berichten in de mappen. Ga als volgt te werk:

- Klik op de knop 'Zoeken' (zie Figuur 122) om berichten te doorzoeken op trefwoorden in de afzender, het onderwerp of de inhoud van de berichten.

Figuur 124: Webmail: Zoek naar berichten

9.2.4 Berichten maken en versturen

Het is ook erg eenvoudig om zelf berichten aan te maken en te versturen.

- Klik op de knop ‘Bericht maken’ (zie Figuur 123) om een tekst schrijven en bijlagen toe te voegen.

Figuur 125: Webmail: Bericht samenstellen

9.3 Vragen stellen over Kennisnet Webmail

U kunt met vragen over Kennisnet Webmail terecht bij:

Telefoon: 0800 – kennisnet
(0800 – 536 64 76 38)
optie 1, - ‘algemene vraag’
daarna optie 2, - ‘kennisnetdiensten’
Fax: 070 – 888 15 93
Mailadres: servicedesk@nltree.nl

10. Kennisnet Webhotel

Kennisnet biedt met Kennisnet Webhotel de mogelijkheid om met uw internet-browser, zoals Microsoft Internet Explorer of Netscape Navigator (zie deel III), de website te beheren die uw organisatie bij kennisnet heeft aangevraagd. Het maakt daarbij niet uit van welk toegangsprotocol u gebruikmaakt. Zowel het protocol van FrontPage, dat van FTP als dat van HTTP-put worden ondersteund.

Met Kennisnet Webhotel kunt u de website (ook wel 'rootweb' genoemd) opdelen in aparte secties (subwebs) met bijbehorende subweb-beheerders. Verder bepaalt u toegangs- en lees/schrijfrechten voor uw website en koppelt deze aan gebruikersgroepen van uw organisatie uit de Kennisnet Gebruikersadministratie (zie hoofdstuk 8).

10.1 De eigen website van uw organisatie

10.1.1 De eigen website van de organisatie bekijken

De website die u gaat beheren met het webhotel, is al beschikbaar. Met de internet-browser (zie deel III) kunt u deze website zowel vanaf kennisnet als vanaf internet bekijken op het adres http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/. Indien u een eigen domeinnaam hebt aangevraagd, zal in de naam van uw website, indien deze naam is toegekend en doorgevoerd in de systemen van kennisnet, de <domeinnaam> zijn opgenomen.

10.1.2 Scripts gebruiken

Voor gebruikers van het standaardweb is een aantal scripts beschikbaar gesteld om te gebruiken op uw website. De scripts zijn te gebruiken voor:

- formulieren: om invulformulieren te versturen;
- paginateller: om te tellen hoeveel personen uw web-pagina hebben bezocht;
- prikbord: waar gebruikers berichtjes kunnen plaatsen.

Uitleg over het gebruik van de scripts en voorbeelden vindt u op het adres:

http://www.nltree.nl/scripts.

10.2 Over Kennisnet Webhotel

Kennisnet Webhotel is ontworpen om organisaties hun websites op een efficiënte wijze te laten beheren. Dit is met name van belang bij complexe websites met veel en gevarieerd onderhoud. De hoofdbeheerder (ICT-coördinator) kan met behulp van webhotel een deel van dit onderhoud uitbesteden aan andere beheerders, die verantwoordelijk worden voor specifieke delen van de website, ofwel subwebs. De hoofdbeheerder heeft automatisch lees- en schrijfrechten voor de hele website.

Kennisnet Webhotel maakt optimaal gebruik van de Kennisnet Gebruikersadministratie. Gebruikersgroepen die in de gebruikersadministratie zijn aangemaakt, kunnen worden gekoppeld aan subwebs van de website door ze lees- of lees/schrijfrechten te geven. Zo kunnen verschillende subwebs op verschillende doelgroepen worden afgestemd. Voorwaarde is dus wel dat u, als ICT-coördinator, gebruikers en gebruikersgroepen in de gebruikersadministratie hebt aangemaakt (zie hoofdstuk 8).

Voorbeeld van lees- en schrijfrechten: de 'homepage van klas 1a' (een subweb) op de website van uw organisatie is alleen in te zien door gebruikersgroep 'klas 1a'. Of, ander voorbeeld: alleen leden van de directie mogen schrijven op de 'nieuwspagina's' (een andere subweb) voor de gebruikersgroep 'docenten'.

De beheermogelijkheden van Kennisnet Webhotel vervangen de standaardmogelijkheden van FrontPage om lees- en schrijfrechten toe te kennen. Beheerders die hun website onderhouden met FrontPage kunnen dus geen gebruikmaken van deze standaard FrontPage-mogelijkheden (lees meer over FrontPage in Bijlage C van Deel VII).

Kennisnet Webhotel is met de internet-browser te vinden op het adres: http://webhotel.kennisnet.nl. Hoe u inlogt, leest u in paragraaf 10.2.3. Het webhotel bevat diverse web-pagina's die via opties uit een hoofdmenu bereikbaar zijn.

10.2.1 Enkele tips

- Om gebruiksrechten aan gebruikers te kunnen geven, moeten deze gebruikers zijn aangemaakt in de Kennisnet Gebruikersadministratie, die ook bereikbaar is via optie 3 in het hoofdmenu van het webhotel. (Zie hoofdstuk 8 voor meer informatie over de gebruikersadministratie.)
- Scholen met een eigen mailserver kunnen er voor gekozen hebben om gebruikers aan te maken zonder mailadres (zie hoofdstuk 8).
- Log altijd uit via de optie 'Logout' in het hoofdmenu van het webhotel als u klaar bent met uw wijzigingen in webhotel. Zo worden uw wijzigingen op een veilige manier opgeslagen.

10.2.2 De diverse webhotel-gebruikers en hun mogelijkheden

Hoofdbeheerder:	Kan subwebs en subwebbeheerders aanmaken, wijzigen en verwijderen. Kan gebruikersgroepen aan subwebs toevoegen en verwijderen. De hoofdbeheerder is bij aanmaak altijd de ICT-coördinator. De hoofdbeheerder ziet als enige de optie 'hoofdbeheerder wijzigen'. Met behulp van deze optie kan hij/zij een nieuwe hoofdbeheerder aanstellen, die vervolgens als enige alle bovengenoemde rechten krijgt. De hoofdbeheerder kan niet verwijderd worden door andere beheerders.
Subwebbeheerder:	Heeft lees- en schrijfrecht voor alleen zijn/haar subweb(s). Dit kan ook de rootweb zijn, als de hoofdbeheerder hem daartoe rechten heeft gegeven. Kan sub-subwebs en mede-subwebbeheerders aanmaken, wijzigen en verwijderen. Kan gebruikersgroepen aan subwebs toevoegen en verwijderen.
Gebruikersgroepen:	Hebben alleen lees- en schrijfrecht voor hun eigen subweb(s). Leden van een groep worden in de Kennisnet Gebruikersadministratie aan de groep toegevoegd.

10.2.3 Op Kennisnet Webhotel inloggen

Voor het beheren van websites en subwebs moet u inloggen op Kennisnet Webhotel:

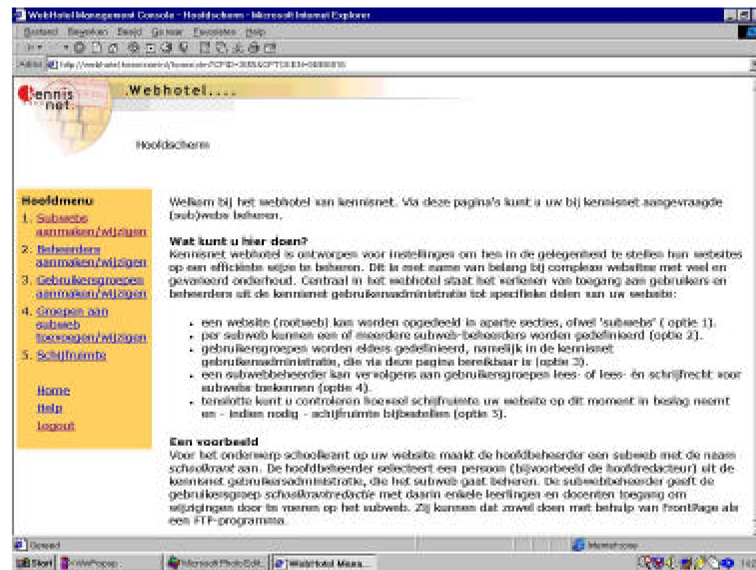
- Start de internet-browser.
- Ga naar het adres http://webhotel.kennisnet.nl/.

Op de web-pagina verschijnt het volgende venster.

Figuur 126: Webhotel aanmelden

- Voer in het veld 'Gebruikersnaam' uw gebruikersnaam in.
- Voer in het veld 'Wachtwoord' uw wachtwoord in.
- Klik op de knop 'Aanmelden'.

De volgende web-pagina verschijnt.



Figuur 127: Webhotel: Hoofdscherm

Vanuit deze web-pagina kunt u door het aanklikken van opties in het hoofdmenu alle noodzakelijke beheeractiviteiten uitvoeren. In de komende paragrafen worden ze achtereenvolgens behandeld.

Let op!

Om veiligheidsredenen blijft een webhotel-pagina maximaal 1 uur actief terwijl u deze niet gebruikt. Daarna moet u opnieuw op het webhotel inloggen.

10.2.4 Opmerking vooraf voor hoofdbeheerders

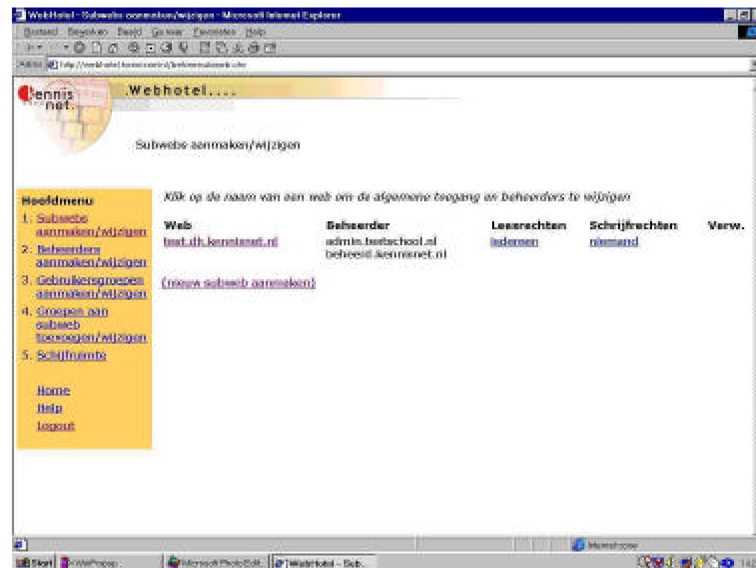
- Als u voor het eerste keer werkt met webhotel, maakt u allereerst één subweb aan en voegt u zichzelf daar als beheerder aan toe. Daarna kunt u andere beheerders en subwebs toevoegen.
- In het huidige webhotel-systeem kunt u alleen een subweb aanmaken indien u daaraan een beheerder koppelt. Omgekeerd kunt u alleen beheerders aanmaken als u daaraan een subweb koppelt.
- U ziet uzelf telkens nog wel in de lijst van beschikbare beheerders terug. Daarbij kunt u ervoor kiezen om alleen u zelf beheerder te maken van een subweb. Indien u een andere beheerder aanstelt, wordt u automatisch medebeheerder. In beide gevallen kunt u daarna niet meer worden verwijderd van subwebs, tenzij u zelf een andere hoofdbeheerder aanstelt.

10.3 Optie 1: Subwebs aanmaken/wijzigen/verwijderen

Als u subwebs wilt aanmaken, wijzigen of verwijderen, doet u het volgende:

- Klik in een webpagina van het webhotel (bijvoorbeeld die van Figuur 127) in het hoofdmenu op ‘Subwebs aanmaken/wijzigen’.

De volgende web-pagina verschijnt, met een overzicht van alle subwebs met per subweb de bijbehorende beheerders.



Figuur 128: Webhotel: Subwebs aanmaken/wijzigen

U kunt via deze web-pagina de volgende taken uitvoeren:

- nieuwe subwebs aanmaken
- subwebs wijzigen
- subwebs verwijderen

10.3.1 Nieuwe subwebs aanmaken

- Klik in Figuur 128 op '(nieuw subweb aanmaken)'.

De volgende web-pagina verschijnt.



Figuur 129: Webhotel: Subweb aanmaken

- Stap 1: indien uw organisatie meerdere domeinnamen heeft: selecteer dan achter het veld 'Schooldomein of subweb:' de gewenste domeinnaam uit de keuzelijst.

Indien uw organisatie één domeinnaam heeft, is deze standaard al ingevuld.

Let op!

Het hierna te bespreken veld ‘Subweb:’ is gevoelig voor hoofd- en kleine letters, dus “Test” is een ander subweb dan “teST”.

- Stap 2: voer in het veld ‘Subweb:’ de naam van de nieuwe subweb in.

  Deze naam wordt straks door het systeem verder aangevuld. Voorbeeld: u voert als naam “test” in en het subweb krijgt automatisch de aangevulde naam “schoolnaam.plaatsnaam.kennisnet.nl/test”.

- Stap 3: alle beschikbare beheerders worden automatisch getoond in het selectieblok ‘Beschikbare beheerders’.

  - Selecteer met uw muis de beheerder(s) die u het nieuwe subweb wilt laten beheren.
  - Klik op ‘voeg selectie toe>’. De beheerders verschijnen nu in het blok ‘Beheerders van dit subweb’.

  U kunt ook in één keer alle beschikbare beheerders toevoegen door te klikken op ‘voeg alles toe>>’.

  Omgekeerd kunt u ook weer beheerders van het subweb verwijderen met ‘<verwijder selectie’ of ‘<<verwijder alles’.

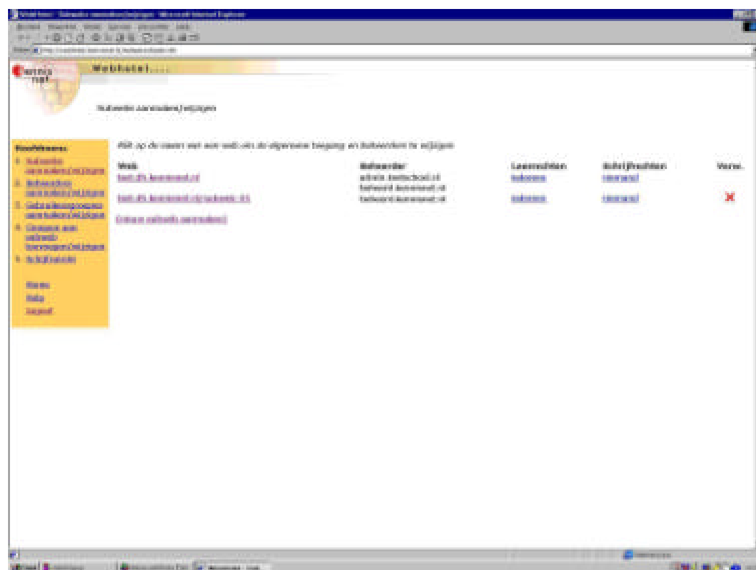
- Stap 4: indien u uw subweb wilt afschermen: selecteer het aanvinkvakje ‘Subweb afschermen?’.

  De subweb is dan alleen via een inlogscherm met gebruikersnaam/wachtwoord bereikbaar voor diegenen aan wie u toegang geeft. Als u wilt dat iedereen met een internet-browser de subweb kan lezen, selecteert u het aanvinkvakje niet.

- Stap 5: als u alles wat u bij de voorgaande stappen hebt ingevoerd of geselecteerd, wilt opslaan: klik op de knop ‘Opslaan’.

  Als u *niets* wilt opslaan: klik op de knop ‘Annuleren’.

De volgende web-pagina verschijnt, waar onder ‘Web’ de nieuwe subweb staat toegevoegd (als voorbeeld ziet u “test.dh.kennisnet.nl/subweb-01”).



Figuur 130: Webhotel: Subwebs aanmaken/wijzigen (met nieuwe subweb)

10.3.2 Subwebs wijzigen

- Klik in de web-pagina als die van Figuur 130 op een van de onderstreepte subwebs onder ‘Web’.

De volgende web-pagina verschijnt. De naam van het aangeklikte subweb is standaard ingevuld achter ‘Subweb:’.



Figuur 131: Webhotel: Subweb wijzigen

- Stap 1: alle beschikbare beheerders worden automatisch getoond in het selectieblok ‘Beschikbare beheerders’.
  - Selecteer met uw muis de beheerder(s) die u de subweb wilt laten beheren.
  - Klik op ‘voeg selectie toe>’. De beheerders verschijnen nu in het blok ‘Beheerders van dit subweb’.

  U kunt ook in één keer alle beschikbare beheerders toevoegen door te klikken op ‘voeg alles toe>>’.

  Omgekeerd kunt u ook weer beheerders van het subweb verwijderen met ‘<verwijder selectie’ of ‘<<verwijder alles’.
- Stap 2: indien u uw subweb wilt afschermen: selecteer het aanvinkvakje ‘Subweb afschermen?’.

  De subweb is dan alleen via een inlogscherm met gebruikersnaam/wachtwoord bereikbaar voor diegenen aan wie u toegang geeft. Als u wilt dat iedereen met een internet-browser de subweb kan lezen, selecteert u het aanvinkvakje niet.
- Stap 3: als u alles wat u bij de voorgaande stappen hebt ingevoerd of geselecteerd, wilt bewaren: klik op de knop ‘Opslaan’.

  Als u *niets* wilt opslaan: klik op de knop ‘Annuleren’.

10.3.3 Subwebs verwijderen

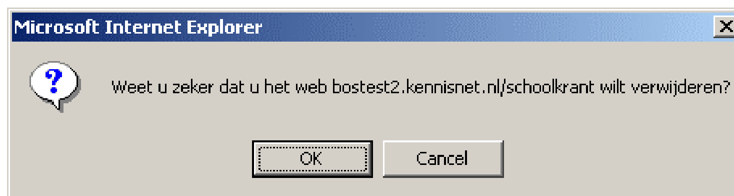
In een web-pagina als die van Figuur 130 kan het volgende staan:

Web	Beheerder	Leesrechten	Schrijfrechten	Verw.
bostest2.kennisnet.nl	admin.bostest2.ede	iedereen	niemand	
bostest2.kennisnet.nl/schoolkrant	admin.bostest2.ede test	iedereen	groepschoolkrant	✕

Figuur 132: Webhotel: Subweb verwijderen (detail)

- Klik op het rode kruisje achter het subweb dat u wilt verwijderen.

Er verschijnt een waarschuwingsmelding, bijvoorbeeld:



Figuur 133: Webhotel: Subweb verwijderen, waarschuwing

- Indien u de subweb definitief wilt verwijderen: klik op de knop ‘OK’.
- Indien u het subweb *niet* wilt verwijderen: klik op de knop ‘Cancel’.

10.4 Optie 2: Beheerders aanmaken/wijzigen/verwijderen

Als u beheerders van subwebs wilt aanmaken, wijzigen of verwijderen, doet u het volgende:

- Klik in een webpagina van het webhotel (bijvoorbeeld die van Figuur 127) in het hoofdmenu op ‘Beheerders aanmaken/wijzigen’.

De volgende web-pagina verschijnt, met een overzicht van alle beheerders met per beheerder de bijbehorende subwebs.



Figuur 134: Webhotel: Beheerders aanmaken/wijzigen

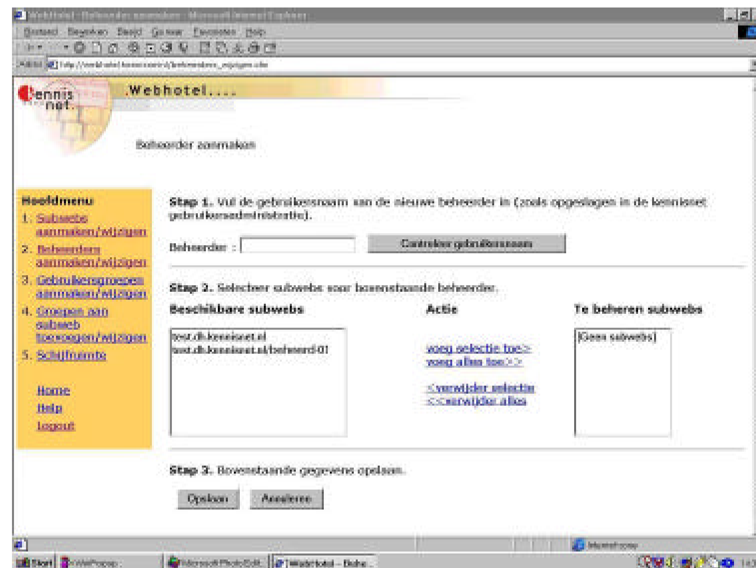
U kunt via deze web-pagina de volgende taken uitvoeren:

- beheerders aanmaken
- beheerders wijzigen
- beheerders verwijderen

10.4.1 Beheerders aanmaken

- Klik in een web-pagina als van Figuur 134 op ‘(beheerder aanmaken)’.

De volgende web-pagina verschijnt.



Figuur 135: Webhotel: Beheerder aanmaken

- Stap 1: voer in veld 'Beheerder:' de gebruikersnaam van de nieuwe beheerder in. Dit moet een bestaande gebruikersnaam uit de Kennisnet Gebruikersadministratie zijn.
    - Om te checken of de naam in de Kennisnet Gebruikersadministratie voorkomt en u deze correct hebt ingevuld: klik op de knop 'Controleer gebruikersnaam'.
- Stap 2: alle beschikbare subwebs worden automatisch getoond in het selectieblok onder 'Beschikbare subwebs'.
    - Selecteer met uw muis de subwebs in het selectieblok, die u wilt toevoegen aan de bij stap 1 ingevoerde beheerder.
    - Klik op 'voeg selectie toe>'. De subwebs verschijnen nu in het blok onder 'Te beheren subwebs'.

  U kunt ook in één keer alle beschikbare subwebs toevoegen door te klikken op 'voeg alles toe>>'.

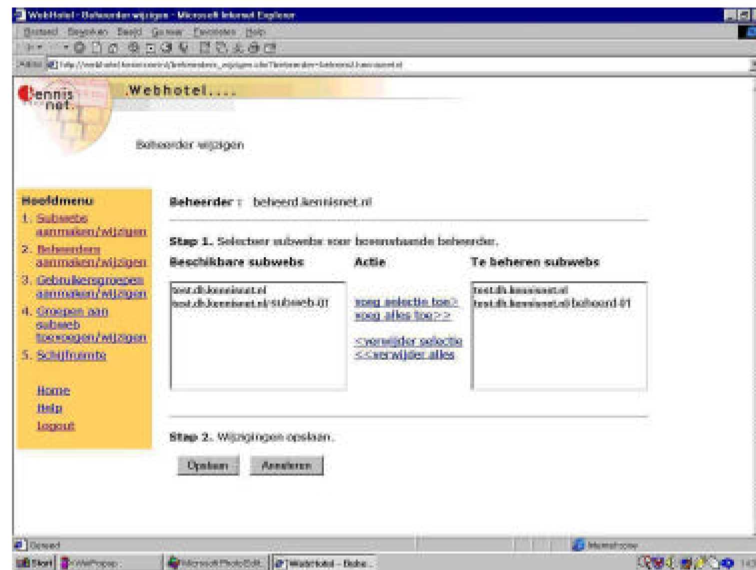
  Omgekeerd kunt u ook weer subwebs van de beheerder verwijderen met '<verwijder selectie' of '<<verwijder alles'.
- Stap 3: als u alles wilt opslaan wat u onder de vorige stappen hebt ingevoerd of geselecteerd: klik op de knop 'Opslaan'.

  Als u *niets* wilt opslaan: klik op de knop 'Annuleren'.

10.4.2 Beheerders wijzigen

- Klik in de web-pagina als die van Figuur 130 op een van de onderstreepte beheerders onder 'Beheerder'.

De volgende web-pagina verschijnt. De naam van het aangeklikte beheerder is standaard ingevuld achter 'Beheerder:'.



Figuur 136: Webhotel: Beheerder wijzigen

- Stap 1: alle beschikbare subwebs worden automatisch getoond in het selectieblok 'Beschikbare subwebs'.
  - Selecteer met uw muis de subwebs die u wilt laten beheren door de ingevulde beheerder.
  - Klik op 'voeg selectie toe>'. De subwebs verschijnen nu in het blok 'Te beheren subwebs'.

    U kunt ook in één keer alle beschikbare subwebs toevoegen door te klikken op 'voeg alles toe>>'.

    Omgekeerd kunt u ook weer subwebs van de beheerder verwijderen met '<verwijder selectie' of '<<verwijder alles'.
- Stap 2: als u alles wat u bij de voorgaande stap hebt geselecteerd wilt opslaan: klik op de knop 'Opslaan'.

  Als u *niets* wilt opslaan: klik op de knop 'Annuleren'.

10.4.3 Beheerders verwijderen

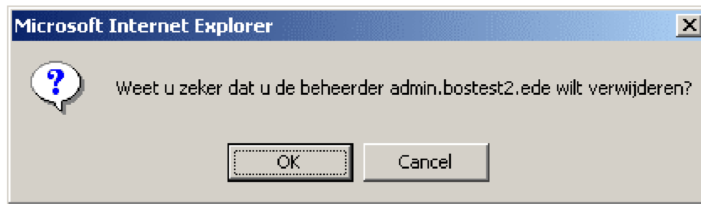
In een web-pagina als die van Figuur 134 kan het volgende staan:



Figuur 137: Webhotel: Beheerder verwijderen (detail)

- Klik op het rode kruisje achter de beheerder die u wilt verwijderen.

Er verschijnt een waarschuwingsmelding, bijvoorbeeld:



Figuur 138: Webhotel: Beheerder verwijderen, waarschuwing

- Indien u de beheerder definitief wilt verwijderen: klik op de knop ‘OK’
- Indien u het beheerder *niet* wilt verwijderen: klik op de knop ‘Cancel’.

10.5 Optie 3: Gebruikersgroepen aanmaken/wijzigen

Gebruikersgroepen maakt u niet aan in het webhotel zelf, maar met behulp van de web-pagina’s voor de Kennisnet Gebruikersadministratie (zie hoofdstuk 8). Deze web-pagina’s zijn wel via webhotel bereikbaar.

Als u via het webhotel gebruikersgroepen wilt aanmaken of wijzigen, doet u het volgende:

- Klik in een webpagina van het webhotel (bijvoorbeeld die van Figuur 127) in het hoofdmenu op ‘Gebruikersgroepen aanmaken/wijzigen’.

De volgende web-pagina verschijnt.



Figuur 139: Webhotel: Gebruikersgroepen aanmaken/wijzigen

- Klik op ‘Start de kennisnet beheersinterface van de gebruikersadministratie’.

Er verschijnen enkele meldingen die aangeven dat u contact maakt via een beveiligde verbinding:

- Klik telkens op de knop ‘OK’.

Ten slotte verschijnt het volgende venster waarin u opnieuw dient in te loggen met uw gebruikersnaam/wachtwoord, waarna wordt gecontroleerd of u rechten hebt om gebruikersgroepen aan te maken of te wijzigen.

Let op!

Lees- en schrijfrechten in webhotel zijn gescheiden van lees- en schrijfrechten in de webpagina's voor de gebruikersadministratie! Wanneer u dus toegang hebt tot het webhotel, betekent dit niet automatisch dat u ook toegang hebt tot de gebruikersadministratie en omgekeerd.



Figuur 140: Webhotel: Netwerkwachtwoord opgeven

Als u de juiste rechten bezit, kunt u vervolgens gebruikersgroepen aanmaken en wijzigen (zie paragraaf 8.11).

Nadat u uitlogt uit de web-pagina's voor de Kennisnet Gebruikersadministratie komt u automatisch terug in een web-pagina van het webhotel, waarna u daar verder kunt gaan met het beheer van uw website.

Let op!

Om veiligheidsredenen blijft de webhotel-pagina maximaal 1 uur actief terwijl u deze niet gebruikt. Daarna moet u opnieuw op het webhotel inloggen.

10.6 Optie 4: Groepen aan subweb toevoegen/wijzigen

Gebruikersgroepen van uw organisatie met *leesrecht* kunnen subwebs bekijken via hun internet-browser, een FTP-programma of met FrontPage. Zij kunnen niets aan het subweb wijzigen (uploaden). Gebruikersgroepen met *lees- en schrijfrecht* kunnen zowel lezen als wijzigen.

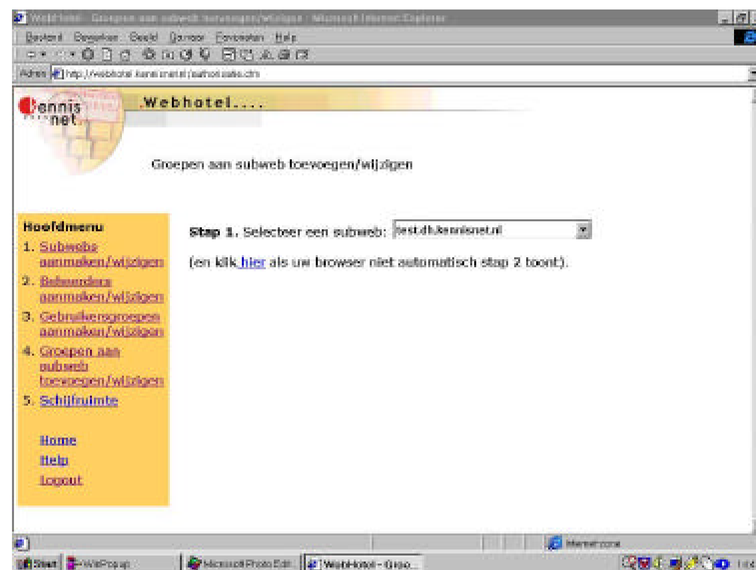
Let op!

Als u een subweb hebt afgeschermd (zie paragraaf 10.3.1 of 10.3.2), dan betekent dat automatisch dat gebruikersgroepen (welke rechten ze ook bezitten) bij dat subweb moeten inloggen met behulp van gebruikersnaam/wachtwoord via een inlogscherm.

Het toekennen van lees en/of schrijfrechten aan een gebruikersgroep noemen we het toevoegen van een gebruikersgroep aan dat subweb. Als u rechten aan gebruikersgroepen van uw organisatie wilt toekennen of iets aan de rechten wilt wijzigen, doet u het volgende:

- Klik in een webpagina van het webhotel (bijvoorbeeld die van Figuur 127) in het hoofdmenu op 'Groepen aan subweb toevoegen/wijzigen'.

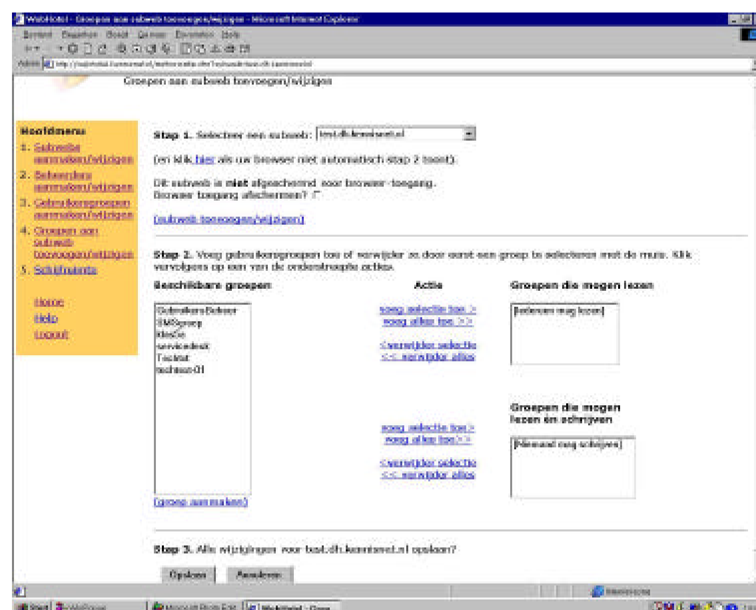
De volgende web-pagina verschijnt.



Figuur 141: Webhotel: Groepen aan subweb toevoegen/wijzigen (onvolledig)

- Klik op ‘hier’, indien nodig.

De volgende webpagina verschijnt.



Figuur 142: Webhotel: Groepen aan subweb toevoegen/wijzigen (volledig)

- Stap 1: selecteer uit de keuzelijst met alle subwebs het subweb waaraan u gebruikersgroepen wilt toevoegen (die u rechten wilt toekennen).
- Het aanvinkvakje ‘Browser toegang afschermen?’ is aangevinkt wanneer het subweb is afgeschermd. U kunt dat van hieruit, indien gewenst, ongedaan maken of juist de afscherming activeren. Het subweb is dan alleen via een inlogscherm met gebruikersnaam/wachtwoord bereikbaar voor diegenen aan wie u toegang geeft. Klik voor dit alles op ‘(subweb toevoegen/wijzigen)’. Een web-pagina als van Figuur 130 verschijnt, zie verder paragraaf 10.3.2.

- Stap 2: alle beschikbare gebruikersgroepen uit de Kennisnet Gebruikersadministratie worden automatisch getoond in het selectieblok 'Beschikbare groepen'.
  - Selecteer met uw muis de groepen die u wilt toevoegen aan het subweb (rechten wilt geven).
  - Als u alleen *leesrechten* wilt geven: klik op 'voeg selectie toe>' links van het blok 'Groepen die mogen lezen'. Deze groepen verschijnen nu in het blok 'Groepen die mogen lezen'. (U kunt ook in één keer alle beschikbare groepen leesrechten geven door te klikken op 'Voeg alles toe>>'. Omgekeerd kunt u ook weer groepen de leesrechten ontnemen met '<verwijder selectie' of '<<verwijder alles'.)
  - Als u *lees- en schrijfrechten* wilt geven: klik op 'voeg selectie toe>' links van het blok 'Groepen die mogen lezen èn schrijven'. Deze groepen verschijnen nu in het blok 'Groepen die mogen lezen èn schrijven'. (U kunt ook in één keer alle beschikbare groepen lees- en schrijfrechten geven door te klikken op 'Voeg alles toe>>'. Omgekeerd kunt u ook weer groepen de lees- en schrijfrechten ontnemen met '<verwijder selectie' of '<<verwijder alles'.)
- Stap 3: als u alle rechten die u in de voorgaande stappen hebt toegekend, wilt opslaan: klik op de knop 'Opslaan'.

  Als u de rechten *niet* wilt opslaan: klik op de knop 'Annuleren'.

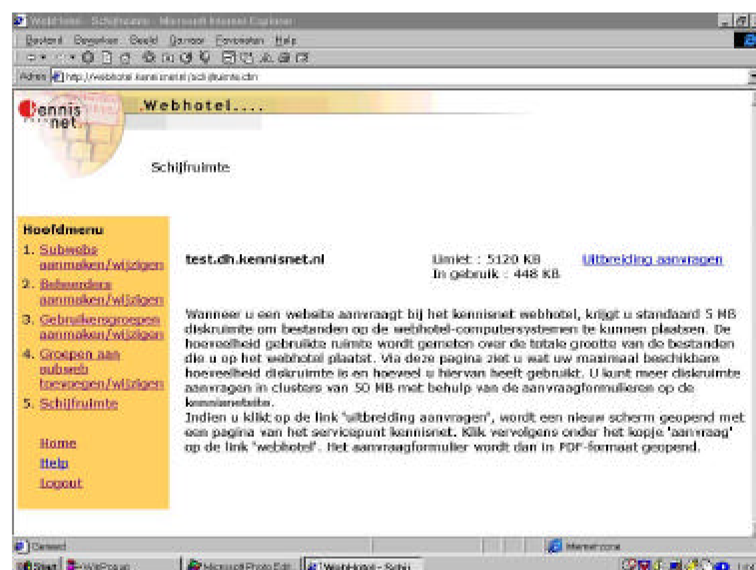
10.7 Optie 5: Schijfruimte

Wanneer u een website aanvraagt bij Kennisnet Webhotel, krijgt u standaard 5 MB schijfruimte om bestanden op de computersystemen van het webhotel te kunnen plaatsen. De hoeveelheid schijfruimte die uw organisatie daadwerkelijk gebruikt, wordt gemeten over de totale grootte van de bestanden die de organisatie op het webhotel plaatst.

Indien u informatie over de schijfruimte wilt of om uitbreiding wilt vragen, doet u het volgende:

- Klik in een webpagina van het webhotel (bijvoorbeeld die van Figuur 127) in het hoofdmenu op 'Schijfruimte'.

De volgende web-pagina verschijnt.



Figuur 143: Webhotel: Schijfruimte

U ziet de domeinnaam. Bij het veld 'Limiet' ziet u wat de maximaal beschikbare schijfruimte van het domein is en bij 'In gebruik' hoeveel uw organisatie hiervan heeft gebruikt.

U kunt meer schijfruimte aanvragen, in clusters van 50 MB, met behulp van de aanvraagformulieren op kennisnet:

- Klik op 'Uitbreiding aanvragen'.

Het volgende formulier in PDF-formaat (te lezen met Adobe Acrobat Reader) verschijnt.

Figuur 144: Webhotel: formulier 'Wijzigingen webhotel voor instellingen' (detail)

- Druk het formulier af.
- Vul het formulier in.
- Verstuur het formulier zoals erop vermeld staat.

10.8 Optie Logout

Wanneer u klaar bent met uw activiteiten in het Kennisnet Webhotel, is het voor het veilig opslaan van alle gegevens het beste dat u het webhotel correct verlaat:

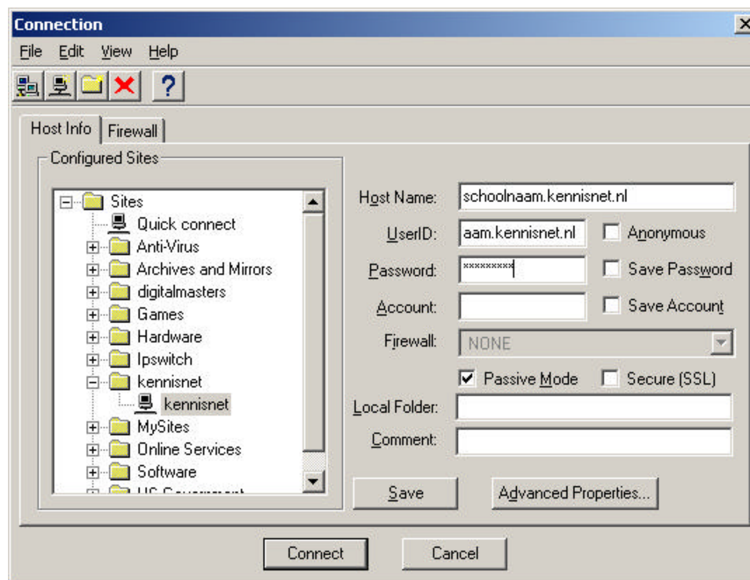
- Klik in een webpagina van het webhotel (bijvoorbeeld die van Figuur 127) in het hoofdmenu op 'Logout'.

10.9 Aanvullende informatie over Webhotel

10.9.1 Op de website inloggen met FTP

Om bestanden van uw computer naar de servers van webhotel te kopiëren (uploaden), moet u gebruikmaken van een FTP-programma (File Transfer Protocol, zie deel III). Een FTP-programma maakt verbinding tussen uw computer en de host-computer, in dit geval de webserver van webhotel.

Om de verbinding (connection) te maken, moet u bijvoorbeeld een scherm als het volgende invullen.



Figuur 145: WS_FTP: Connection, Hostinfo

Om verbinding te maken moet u de volgende gegevens invullen:

- Voer in het veld 'Hostname' in:
  "`schoolnaam.plaatsnaam.kennisnet.nl`" of "`www.schooldomein.nl`"
- Voer in het veld 'UserID' in:
  "`gebruikersnaam#schoolnaam.plaatsnaam.kennisnet.nl/subdirectory`" of:
  "`gebruikersnaam#www.schooldomein.nl/subdirectory`". Denk aan het volgende:
  - Het [#]- teken moet worden ingevuld!
  - "Gebruikersnaam" is de naam zoals opgeslagen in de Kennisnet Gebruikersadministratie.
  - Bij "subdirectory" vult u het subweb in waarvoor u lees- en/of schrijfrechten hebt. Hebt u toegang tot de hele website, dan hoeft u geen subdirectory in te vullen en komt u in het rootweb. Van daaruit kunt u alle andere directory's (subwebs) bereiken.
  - Voer in het veld 'Password' in: uw wachtwoord zoals opgeslagen in de Kennisnet Gebruikersadministratie

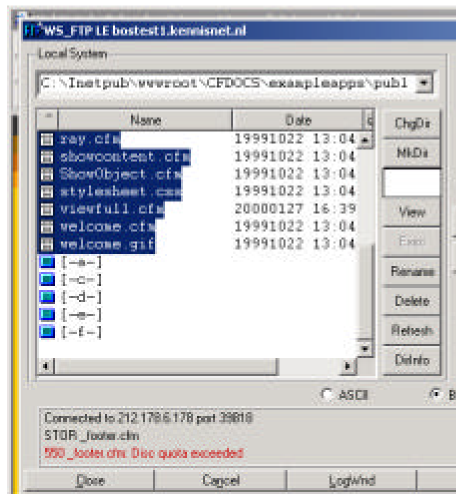
Nadat u deze instellingen hebt ingevoerd, kunt u verbinding maken met de webhotelserver.

Vervolgens krijgt u de directory-structuur van het subweb te zien. Als u schrijfrecht hebt, kunt u bestanden kopiëren naar deze directory's.

10.9.2 Schijfruimte overschrijden

Als de aan uw organisatie toegekende schijfruimte (zie paragraaf 10.7) echt structureel wordt overschreden, wordt het toevoegen van nieuwe bestanden geblokkeerd totdat u bestanden op de website hebt verwijderd.

Na het overschrijden van de toegekende schijfruimte krijgt u een melding als: "disc quota exceeded".

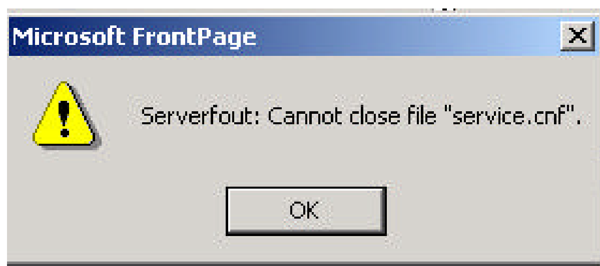


Figuur 146: WS_FTP LE, melding “Disc quota exceeded”

10.9.3 Schijfruimte overschrijden in FrontPage

Als de toegekende diskruimte echt structureel wordt overschreden (zie paragraaf 10.7), dan wordt het toevoegen van nieuwe bestanden geblokkeerd totdat u bestanden op de website verwijdert.

De FrontPage-foutmelding hierover is nogal cryptisch, zoals u ziet.



Figuur 147: Microsoft FrontPage: ‘Serverfout: Cannot close file “service.cnf” (Foutmelding schijfruimte)

Er is dus niets mis met de website: er is echter geen schijfruimte meer.

10.9.4 Op de website inloggen met FrontPage

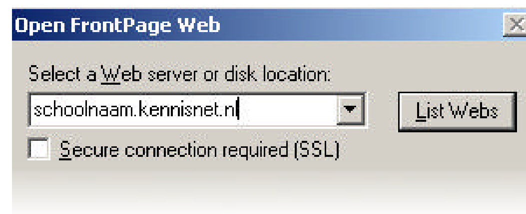
Let op!

Er is verschil tussen de verschillende FrontPage-versies. Hieronder wordt de situatie beschreven voor FrontPage 98 op Windows 98 en FrontPage 2000 op Windows 2000. Hebt u een andere configuratie: neem dan contact op met uw systeembeheerder, indien nodig.

10.9.4.1 FrontPage 98

- Open FrontPage.
- Klik op ‘more webs’.

Vervolgens verschijnt het volgende venster.

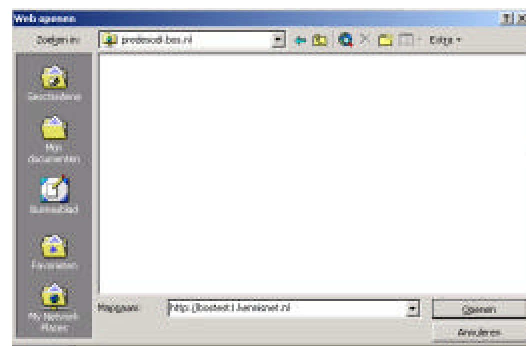


Figuur 148: FrontPage 98, Open FrontPage Web

10.9.4.2 FrontPage 2000

- Open FrontPage.
- Klik op ‘bestand -> open web’.

Vervolgens verschijnt het volgende venster.



Figuur 149: FrontPage 2000, Web openen

- Voer in het veld ‘Mapnaam’ in: het adres van de website van uw organisatie. Bijvoorbeeld: `http://schoolnaam.plaatsnaam.kennisnet.nl`

10.9.4.3 Voor beide versies van FrontPage

- Voer bij ‘www.schooldomein.nl/subdirectory’ in: de subdirectory of het subweb waarvoor u lees-en/of schrijfrechten hebt. Hebt u toegang tot de hele website, dan hoeft u geen subdirectory in te vullen en komt u in het rootweb. Van daaruit kunt u alle andere directory’s (subwebs) bereiken.

Vervolgens wordt u gevraagd om uw gebruikersnaam en wachtwoord op te geven.



Figuur 150: FrontPage: Name and Password Required

- Voer in het veld ‘Name’ in: de gebruikersnaam, zoals opgeslagen in de Kennisnet Gebruikersadministratie

- Voer in het veld 'Password' in: het wachtwoord zoals opgeslagen in de Kennisnet Gebruikersadministratie

U krijgt alleen toegang tot het subweb indien u lees- of lees/schrijfrechten hebt voor het desbetreffende subweb.

Let op!

FrontPage biedt de functie 'list webs' waaronder normaliter in FrontPage aangemaakte subwebs (directory's) worden getoond. Deze functie is uitgeschakeld, omdat u subwebs definieert via het webhotel en niet meer in FrontPage. De in webhotel aangemaakte subwebs worden dus niet getoond onder 'list webs'.

10.9.5 De verschillen tussen een subdirectory en een subweb

Een directory is een submap waarin bestanden geplaatst kunnen worden.

Een subweb is een directory met daaraan gekoppeld gebruikers die lees- of schrijfrechten hebben op die directory.

10.9.6 Webhotel: subdirectory's en subwebs

Webhotel controleert of het subweb al als directory in uw bestandenstructuur bestaat. Is dat het geval, dan krijgt die directory automatisch de status van 'subweb'. Bestaat de directory nog niet, dan verschijnt een waarschuwingsmelding. Als u op de knop 'OK' klikt, wordt een directory met de naam van het subweb aangemaakt.

10.9.7 Via FTP of FrontPage verwijderen van een directory die in webhotel als subweb is gedefinieerd

Hoewel de subdirectory 'fysiek' niet meer bestaat als u deze verwijdert met FTP of ProntPage, blijft deze tijdelijk nog wel zichtbaar als subweb in de lijst met subwebs op het webhotel. Zodra u een actie met het subweb wilt uitvoeren, (wijzigen of verwijderen) registreert het webhotel dat de bijbehorende directory niet meer bestaat en verwijdert het subweb.

10.9.8 Een subweb verwijderen via webhotel.

Na het verwijderen van een subweb met webhotel blijft de bijbehorende directory wel bestaan; alleen de gebruikers met lees- of schrijfrechten worden verwijderd.

Let op!

De directory krijgt nu automatisch de lees- en schrijfrechten van de bovenliggende directory!

10.10 Verklarende woordenlijst

Rootweb	Hoofddirectory (website) behorende bij uw domein
Subweb	Zelfstandige website die onder het hoofddomein valt
Kennisnet Gebruikersadministratie	Centraal gegevensbestand met gebruikers van kennisnet (zie hoofdstuk 8)
FrontPage	Programma waarmee websites onderhouden kunnen worden (zie bijlage C van deel VII)
FTP-programma	Programma waarmee bestanden naar een website gekopieerd kunnen worden (File Transfer Protocol) (zie deel III)
HTTP-put	Protocol waarmee eveneens bestanden naar een website gekopieerd kunnen worden
leesrecht	Toegang om bestanden te raadplegen
schrijfrecht	Toegang om bestanden te wijzigen
schijfruimte	Hoeveelheid beschikbare ruimte voor de website van een organisatie op de computersystemen van webhotel

internet-browser	(Blader)programma waarmee u websites kunt bekijken (Internet Explorer, Netscape) (zie deel III)

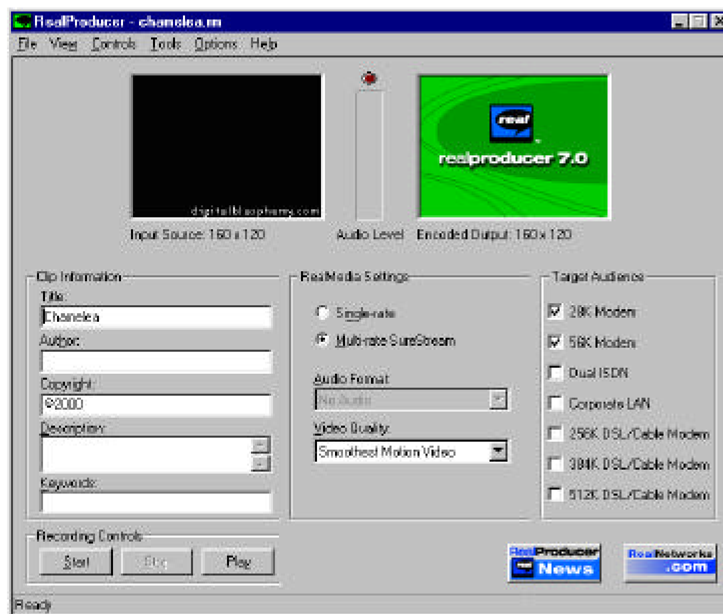
11. Kennisnet Realserver

Kennisnet biedt scholen de mogelijkheid om hun geluid- en filmbestanden via kennisnet af te spelen. Hiervoor wordt gebruik gemaakt van de Real media-server van Kennisnet. Het belangrijkste kenmerk van Real media is dat het een 'streaming' technologie is. Dat heeft als voordeel dat het bestand niet eerst helemaal gedownload hoeft te worden, voordat met afspelen wordt begonnen. Real media maakt daarvoor gebruik van een buffer: eerst worden de data binnengehaald en als er genoeg data binnen zijn, kan het afspelen starten. Een tweede voordeel is dat Real media-bestanden dankzij een speciale compressie-methode relatief klein zijn.

11.1 RealAudio- en RealVideo-bestanden maken

Om geluid of filmpjes om te zetten naar een Real media-bestand, hebt u een zogenoemde Real media-encoder nodig. Dit is een programma waarmee u bijvoorbeeld een ".avi"-filmpje kunt omzetten naar een "RealVideo"-bestand (.rm). U kunt in het programma opgeven welk bestand als bron (source) moet dienen en welke naam u het wilt geven. Het programma converteert het bronbestand dan automatisch naar een Real-formaat met het achtervoegsel ".ra" of ".rm".

Een Real media-encoder zit verwerkt in het product RealProducer van Realnetworks. Van dit product is een gestripte versie gratis te downloaden van de website http://www.real.com/ voor vrij gebruik, via de subpagina http://www.realnetworks.com/products/producer/info.html. Met RealProducer kunt u onder meer bestanden omzetten naar Real media-bestanden en een Real media-bestand opnemen. Hieronder ziet u een venster uit RealProducer.



Figuur 151: RealProducer

11.2 RealAudio- en RealVideo-bestanden 'uploaden' naar de Kennisnet Realserver

Dit gebeurt met een FTP-programma (file transfer protocol, zie deel III). U dient hiervoor uw eigen gebruikersnaam/wachtwoord-combinatie in te voeren, gevolgd door de toevoeging #BRINNOsiteman. Dat is dezelfde combinatie als u voor het 'uploaden' van uw website naar het Kennisnet Webhotel gebruikt. Houdt u er rekening mee dat de FTP-proxy van kennisnet gebruikt moet worden. Uitleg hierover en over de werking van FTP vindt u in Deel III.

Let op 1!

Wat u hier invoert is hoofdlettergevoelig, dus het BRIN-nummer moet in hoofdletters.

Let op 2!

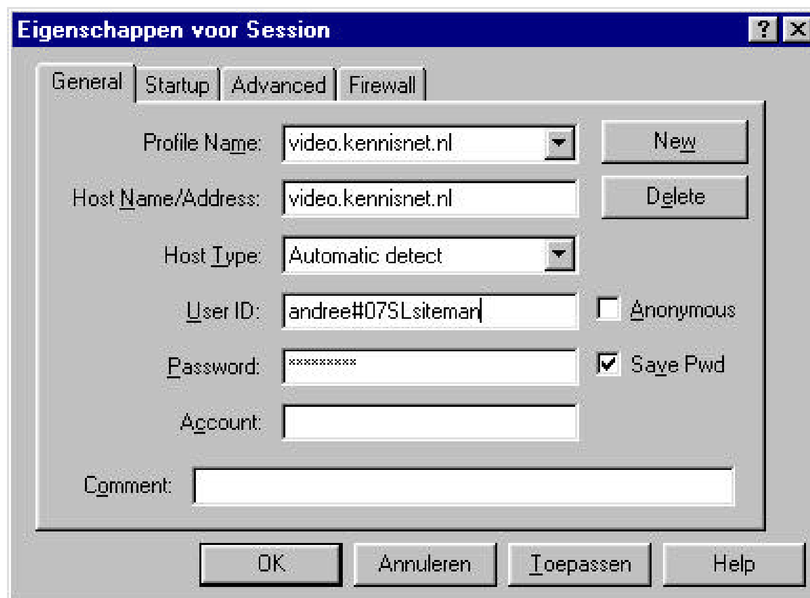
Hier wordt niet de gebruikersnaam/wachtwoord-combinatie bedoeld die u eventueel voor de FrontPage-server gebruikt.

Adres voor het uploaden van de bestanden:	www.video.kennisnet.nl
Gebruikersnaam:	GEBRUIKER#BRINNOsiteman

U komt nu rechtstreeks in uw eigen home-directory terecht.

Adres van 'ge-uploade' RealVideo-bestanden:	`rtsp://video.kennisnet.nl/BRINNO/bestand` (voorbeeld: rtsp://video.kennisnet.nl/07SL/test.rm)

Op dezelfde manier kunt u met uw FTP-programma bestanden verwijderen of hernoemen (zie onderstaande figuur voor een inlog-voorbeeld voor WS-FTP lite).



Figuur 152: WS-FTP lite, Eigenschappen voor Sesion, General

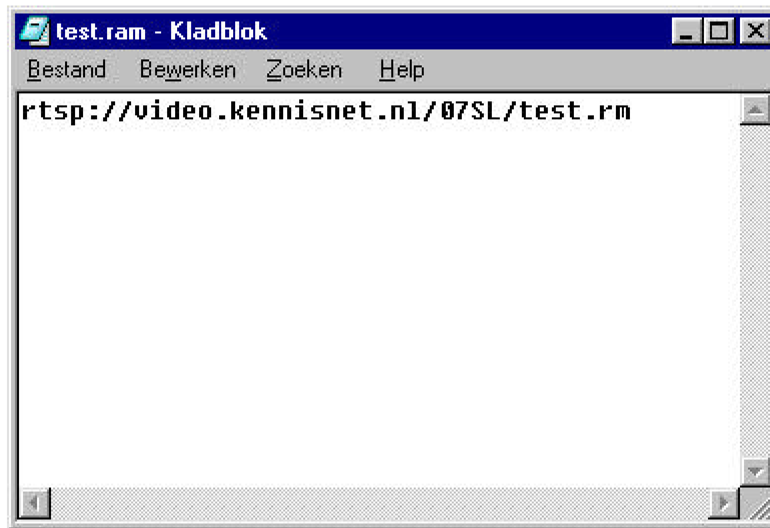
11.3 Een link om RealVideo-bestanden af te spelen

Om een link te maken naar uw RealVideo-bestand, moet u een zogenaamd meta-bestand maken. Dat is een indirecte verwijzing naar het desbetreffende RealVideo-bestand. Als u namelijk een directe link naar een RealVideo-bestand maakt, wil de 'client' (bijvoorbeeld uw pc) het desbetreffende bestand in zijn geheel downloaden en dus niet 'streaming' afspelen.

Een meta-bestand kunt u maken met behulp van Windows Kladblok (Notepad) of een andere eenvoudige tekst-editor:

- Zet in het Kladblok-bestand het precieze internetadres van het desbetreffende RealVideo-bestand.
- Sla dit op als een bestand met de extensie ".ram".

Dit "*.ram"-bestand moet op de webserver komen te staan, niet op de videoserver. Het "*.ram"-bestand zorgt er vervolgens voor dat de RealPlayer wordt geactiveerd en dat u het RealVideo-bestand 'streaming' kunt bekijken. Het kan er zo uitzien:



Figuur 153: “*.ram”-bestand met Kladblok (Notepad)

Om de Real media-bestanden in een website op te nemen, moet er op een website een hyperlink in de HTML-code gemaakt worden naar dit meta-bestand. Door op de gewenste plek de volgende regel binnen de website op te nemen, ontstaat er een directe link naar het filmpje:

```
<a href=”http://uwdomeinnaam/test.ram”>Klik hier voor video.</a>
```

“uwdomeinnaam” staat hier voor “<schoolnaam>.<plaatsnaam>.kennisnet.nl” als u van de standaard kennisnet-adresgeving gebruikmaakt of bijvoorbeeld “www.domeinnaam.nl” als u over een eigen domeinnaam beschikt.

Op de desbetreffende plek op de website verschijnt nu de tekst ‘Klik hier voor video’. Klik erop en er verschijnt een nieuw venster van RealPlayer.



Figuur 154: RealPlayer gaat afspelen

- Als eerste meldt de RealPlayer dat hij gaat ‘connecten’ met de videoserver.
- Vervolgens verschijnt de melding dat de buffer gevuld wordt en hoe lang het nog duurt voordat de film gaat draaien.

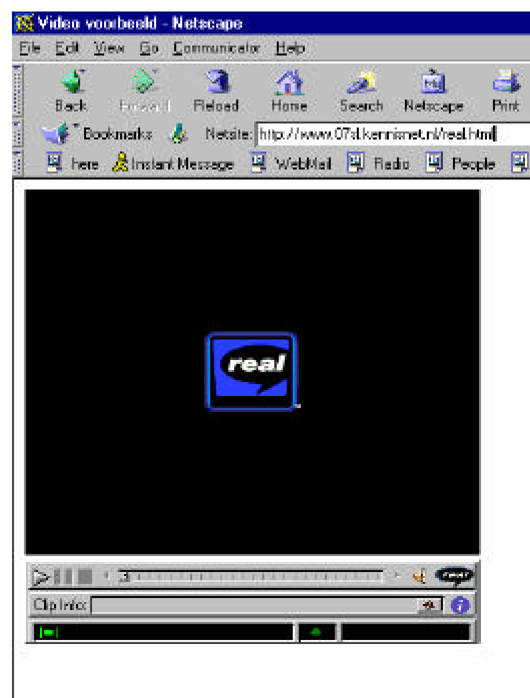
11.4 Mogelijke problemen

Als de ‘connecting’-melding blijft staan en er verder niets gebeurt, controleer dan de instellingen van de RealPlayer. Met name als er binnen kennisnet gewerkt wordt, moeten er een aantal standaard instellingen veranderd worden (proxy -instellingen voor RealPlayer). Deze instellingen vindt u in Deel III.

Als het netwerk zwaar belast is, kan het beeld schokkerig bewegen of zelfs stil staan. In dat geval doet u er verstandig aan om andere netwerk-werkzaamheden tijdelijk te onderbreken, zoals downloaden van grote bestanden of zelfs ‘surfen’. Komt dit vaak voor dan kunt u overwegen uw aansluitcapaciteit te vergroten.

11.5 RealVideo volledig integreren in een web-pagina

Om RealVideo zodanig te integreren in een web-pagina dat er geen nieuw venster geopend wordt, zijn een aantal HTML-regels nodig.



Figuur 155: RealPlayer: voorbeeld van integratie

Hieronder staat de code voor een voorbeeldbestand. In dit voorbeeld is het Real media-bestand ‘testfilmpje’ genoemd. Vervang dit overal door de naam van uw eigen Real media-bestand en vervang ‘BRINNO’ door het BRIN-nummer van uw instelling.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
  <HEAD>
   <meta name="rnpagelayout" content="embedded">
   <meta name="rnserverpath" content="http://video.kennisnet.nl/BRINNO/">
   <meta name="rnmediafile" content="testfilmpje">
   <meta name="rnmetafile" content="testfilmpje.ram">
   <TITLE>Video voorbeeld</TITLE>
  </HEAD>
<BODY>
        <object classid="clsid:CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA" width="352" height="283" id="video1">
            <PARAM NAME="controls" VALUE="ImageWindow">
                <PARAM NAME="console" VALUE="Clip1">
                <PARAM NAME="autostart" VALUE="false">
                <PARAM NAME="src" VALUE="testfilmpje.ram">
           <embed src="testfilmpje.ram" width="352" height="283" type="audio/x-pn-Realaudio-plugin" console="Clip1"
controls="ImageWindow">
    </object>
        <br>
        <OBJECT ID=video1 CLASSID="clsid:CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA" HEIGHT=65 WIDTH=352>
                <PARAM NAME="controls" VALUE="All">
                <PARAM NAME="console" VALUE="Clip1">
                <EMBED type="audio/x-pn-Realaudio-plugin" CONSOLE="Clip1" CONTROLS="All" HEIGHT=65 WIDTH=352
AUTOSTART=false>
        </OBJECT>
</BODY></HTML>
```

Figuur 156: RealPlayer, HTML-code voor integratie

12. Hulpmiddelen en literatuur voor websites

12.1 Hulpmiddelen voor websites

Op het internet zijn diverse hulpmiddelen te krijgen en is een schat aan informatie te vinden voor het maken van de website van uw organisatie. In deze paragraaf worden enkele interessante tips gegeven.

12.1.1 Informatiebronnen voor websites

- **Het Web Graphics Ontwerpboek** [12] Adres: http://www.lynda.com/.
- **Killersites**[13] Informatie voor webontwerpers. Adres: http://www.killersites.com.
- **Netscape Developer Site** De maker van het bladerprogramma 'Communicator' heeft op een speciale website een grote hoeveelheid informatie over het gebruik van onder meer HTML en JavaScript.

  Adres: http://developer.netscape.com/library/documentation/index.html.

12.1.2 On-line-hulpmiddelen voor websites

Er bestaan enkele interessante websites die u op weg kunnen helpen bij het maken van een goede en mooie website. Hier volgt een rijtje van handige websites.

- **Bryan Livingston's CoolText.com: Online Graphics Generator.** Dit is een gratis dienst waar u kleine plaatjes kunt laten genereren, zoals knopjes, paginakoppen en achtergronden. Voor het maken van deze plaatjes wordt, via een webinterface, gebruikgemaakt van de eveneens gratis software GIMP. Adres: http://www.cooltext.com/.

12.1.3 Software voor websites

- **GNU Image Manipulation Program.** Kortweg 'GIMP' – een handig en krachtig tekenprogramma voor UNIX-systemen, waaronder Linux, en het is gratis te gebruiken onder de voorwaarden van de GNU General Public Licence. Adres: http://www.gimp.org/.
- **The Free Builder Project.** 'Free Builder' is een gratis ontwikkelgereedschap voor Java[tm]. Er zijn distributies beschikbaar voor Windows en UNIX-systemen.
- **Tucows.** Op de websites van Tucows kunt u voor onder meer Windows, Mac OS en Java verschillende hulpmiddelen vinden voor het maken en onderhouden van HTML-pagina's.

12.2 Literatuur voor websites

- Telemark Systems, Inc.; "NT DNS Configuration - using BIND 4.9.3 Release"; Telemark Systems, Inc., april 1996; http://www.telemark.net/~randallg/ntdns.htm.
- Langfeldt, Nicolai <janl@math.uio.no>; "DNS-HOWTO" (Linux HowTo); Langfeldt, Nicolai, 1995-1999; http://metalab.unc.edu/pub/linux/docs/howto/DNS-HOWTO.

[12] Bron: Automatisering Gids, Ten Hagen Stam uitgevers, 's-Gravenhage, vrijdag 12 februari 1999 - nr. 6, bladzijde 17.

[13] Idem

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel V: Geavanceerde instellingen

Indeling van deel V

Sommige scholen, met name diegene die reeds enige ervaring met internet hebben opgebouwd, hebben nogal eens wat vragen en wensen rond het aansluiten van hun eigen apparatuur en voorzieningen. In dit deel gaan we nader op deze wensen in.

In hoofdstuk 13 wordt uitgelegd hoe u een eigen DHCP- of BOOTP-server kunt opzetten.

Hoofdstuk 14 gaat in op zaken rond het opzetten van een eigen DNS-server.

In hoofdstuk 15 wordt uitgelegd hoe u de eigen proxy -server kunt blijven gebruiken.

In hoofdstuk 16 wordt uitgelegd hoe u de eigen lokale mailserver kunt blijven gebruiken.

Hoofdstuk 17 behandelt het onderwerp ‘Een eigen webserver opzetten’.

Hoofdstuk 0 behandelt de IP-adressering op kennisnet en de adresvertaling (Network Address Translation, NAT).

Hoofdstuk 19 behandelt netwerkkoppelingen.

13. Een eigen DHCP- of BOOTP-server opzetten

U kunt een eigen DHCP- of BOOTP-server voor uw organisatie opzetten. Daartoe moet u via het Servicepunt Kennisnet een verzoek indienen: http://servicepunt.kennisnet.nl/.

De voor u beschikbaar gestelde reeks IP-adressen zal uit de centrale DHCP-server worden verwijderd en DHCP-relay zal op de router worden uitgeschakeld. U moet de aan u verstrekte IP-adressen voor kennisnet wel voor uw eigen server gebruiken. Vervolgens kunt u uw eigen DHCP- en/of BOOTP-server starten.

Enkele gegevens die u nodig hebt:

Default gateway	het IP-adres van uw router
DNS-servers	212.178.5.4 en 212.178.5.5

De volgende paragrafen beschrijven de configuratie van DHCP-servers.

Let op!

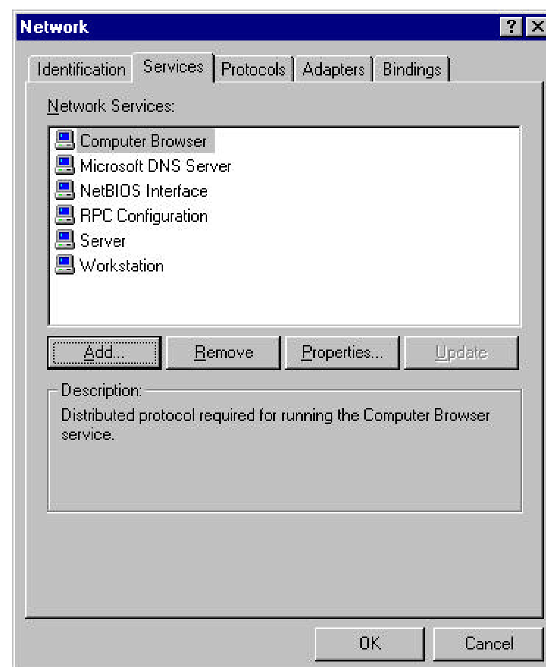
Hierbij wordt gebruikgemaakt van een fictieve reeks IP-adressen.

13.1 Microsoft DHCP-server

De Microsoft DHCP-server is een optioneel onderdeel van Windows NT-server. Mogelijk dient u dit nog als volgt te installeren:

- Open het venster met instellingen.
- Kies dan netwerk (‘Network’).
- Selecteer het tabblad ‘Services’.

Het volgende tabblad wordt geopend.

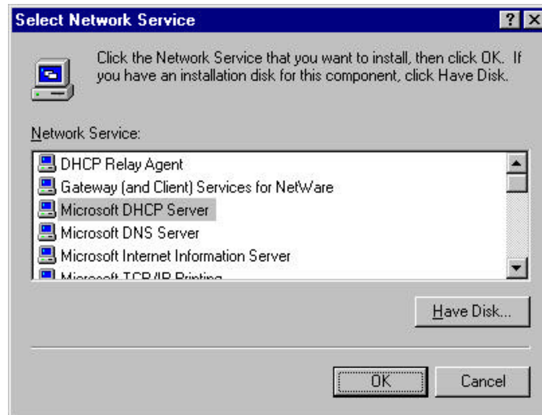


Figuur 157: Microsoft DHCP-server, Network, Services

- Controleer of de DHCP-server in het rijtje voorkomt.

- Indien dit niet het geval is: klik op de knop 'Toevoegen' of 'Add...'.

Het volgende venster verschijnt.



Figuur 158: Microsoft DHCP-server, Select Network Service, Microsoft DHCP server

- Selecteer de DHCP-server. U zult waarschijnlijk worden gevraagd om de CD-ROM te plaatsen voordat u de installatie kunt voltooien.

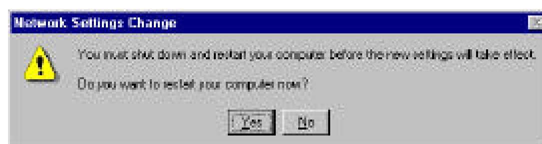
Bij de installatie van de DHCP-server krijgt u waarschijnlijk de volgende waarschuwing dat de NT-server zelf een statisch adres dient te krijgen voordat op deze machine de DHCP-server kan worden gestart.



Figuur 159: Waarschuwing bij installatie DHCP-server

- Klik op de knop 'OK' om de installatie te voltooien.
- Sluit de configuratieschermen.

U krijgt een bericht over herstarten.



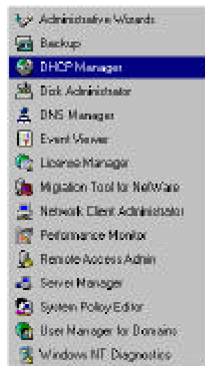
Figuur 160: Network Settings Change: Reboot na installatie

- Klik op de knop 'Yes' om de computer te herstarten.

Na de herstart van de computer dient de DHCP-server te worden geconfigureerd:

- Klik op de Start-knop voor het menu en ga naar de 'Administrative Tools', ofwel de 'Beheerhulpmiddelen'.

U ziet een dergelijk menu.



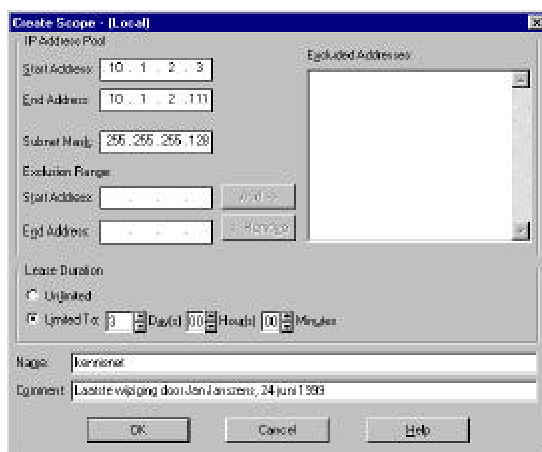
Figuur 161: Administratieve hulpmiddelen

- Open de 'DHCP Manager'.

In het venster dat verschijnt, staat één object: de lokale server.

- Selecteer dit object en kies uit het menu de optie 'Create Scope'.

Er verschijnt een venster waarin u een 'Scope' kunt aanmaken (Create Scope). Hiermee definieert u de uit te delen IP-adressen en aanverwante gegevens.



Figuur 162: Create Scope (Scope aanmaken) (voorbeeld)

- U begint door het eerste en laatste adres uit de IP-reeks op te geven. Vervolgens kunt u het netwerkmasker opgeven. In het voorbeeld is een reeks van in totaal 128 adressen, met netwerkmasker '`255.255.255.128`' gebruikt. Er worden echter slechts 103 adressen voor werkstations uitgedeeld.

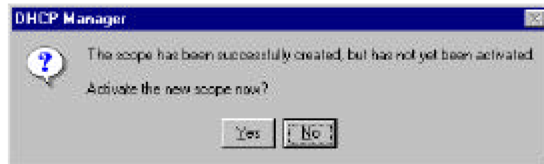
  Let op!

  De start- en eindadressen moeten binnen dezelfde reeks vallen, die mede wordt bepaald door het netwerkmasker!

- Analoog aan de reeks kunt u een aantal subreeksen uitsluiten, bijvoorbeeld omdat u enkele statische adressen aan werkstations wilt uitdelen. Deze reeksen komen in het vak rechts te staan.
- Onder de IP-gegevens kunt u de geldigheidsduur van de uitgedeelde IP-adressen aangeven. Standaard is dit drie dagen. Wanneer er weinig verandering in uw netwerk plaatsvindt, is dit een goede waarde, maar wanneer u veel denkt te veranderen of regelmatig 'bezoekers' hebt, kunt u deze tijd beter korter instellen.

- U kunt bijna onderaan een naam opgeven voor de reeks. Een voor de hand liggende keuze is ‘kennisnet’. Tevens kunt u nog een omschrijving van één regel opgeven voor de scope.

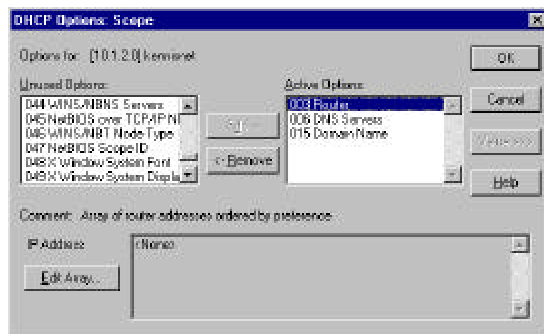
Na het aanmaken van de scope zal worden gevraagd of u deze ook wilt activeren.



Figuur 163: DHCP manager, Scope activeren?

- Het verdient aanbeveling om hier negatief te antwoorden en de scope pas te activeren wanneer u klaar bent met de configuratie van de gegevens. Klik dus op de knop ‘No’.
- Selecteer de lokale scope wederom en kies in het menu ‘Options’ voor ‘Scope’.

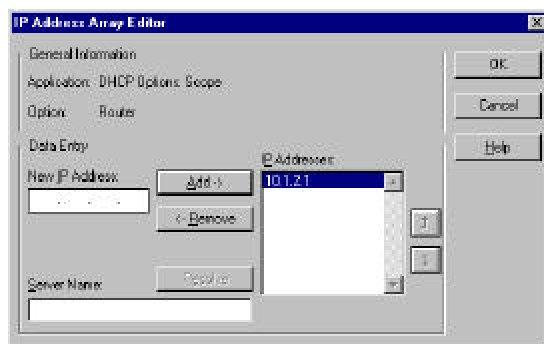
Er verschijnt een venster waarin u nog enkele gegevens voor de scope kunt toevoegen voor wat betreft de uit te delen informatie.



Figuur 164: DHCP Options: Scope

Het wordt aangeraden om uit de linker lijst ten minste de ‘Router’, de ‘DNS Servers’ en ‘Domain Name’ in de rechter lijst op te nemen. Mogelijk hebt u nog behoefte om bijvoorbeeld een eigen WINS-server op te zetten en deze als DHCP-optie mee te geven.

- U kunt nu alle opties configureren door deze te selecteren: klik op de knop ‘Value>>>’ om de bijbehorende gegevens in te vullen.
- Met de knop ‘Edit Array...’ kunt u voor de optie ‘Router’ de gegevens wijzigen in het volgende venster.



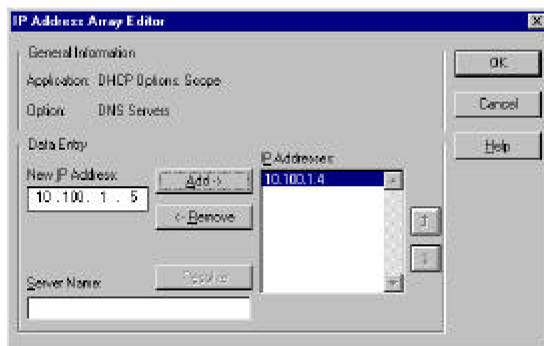
Figuur 165: IP address Array Editor: Router voor een scope

Normaliter is er slechts één gateway in uw lokale netwerk.

- Vul het IP-adres hiervan in onder 'New IP Address:'/'Nieuw IP-adres:' en voeg het met de knop 'Add->' toe aan de lijst.

  Het routeradres dient uiteraard binnen hetzelfde subnet te vallen als de uit te delen IP-adressen en niet te overlappen met de reeks uit te delen IP-adressen.
- Sluit dit venster met de knop 'OK'.

Met de knop 'Edit Array...' kunt u voor de optie 'DNS Servers' de lijst van servers wijzigen in het volgende venster.



Figuur 166: IP address Array Editor: DNS-servers voor een scope

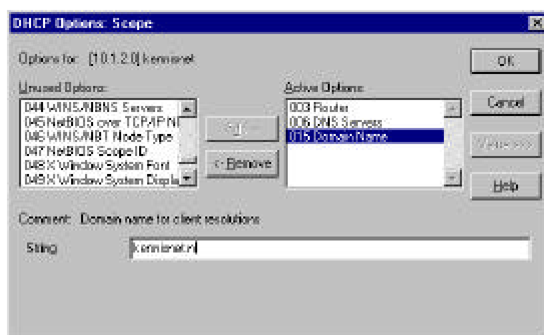
De DNS-servers van kennisnet zijn:

212.178.5.4

212.178.5.5

- Voer in het veld dat verschijnt onder 'New IP Address:' de IP-adressen van de DNS-servers van kennisnet in.
- Klik op de knop 'Add->'. Indien u lokaal een 'Caching DNS Server' hebt, dient u mogelijk dit adres in te geven.

In het optievenster zelf kunt u door de optie 'Domain Name' (of 'Domeinnaam') te selecteren de domeinnaam opgeven.



Figuur 167: DHCP Options: Scope: Domeinnaam voor een scope

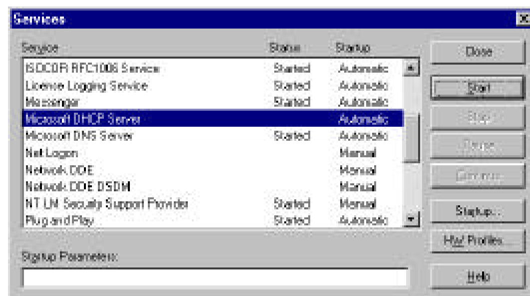
- Selecteer 'Domain Name'.
- Voer achter het veld 'String' de domeinnaam in, namelijk: "kennisnet.nl".
- Sluit vervolgens het venster met de knop 'OK'.
- Activeer eventueel de scope via het menu en sluit de DHCP-manager.

U dient nu eventueel nog de service te activeren met de volgende knop.



Figuur 168: Windows NT Services

Het configuratiescherm voor de ‘Services’ verschijnt.



Figuur 169: Configuratiescherm Services

- Selecteer de ‘Microsoft DHCP Server’.
- Controleer de ‘Status’. Indien de status ‘Started’ is, is de service reeds actief. Anders dient u deze alsnog te starten met ‘Start’, rechts in het venster.
- Controleer de ‘Startup’. De vermelding onder ‘Startup’ dient “Automatic”/“Automatisch” te luiden. Dit kunt u eventueel aanpassen met de knop ‘Startup...’.

13.2 Een eigen DHCP-server in Windows 2000

De DHCP-service in Windows 2000 centraliseert en beheert de toewijzing van TCP/IP-configuratie-informatie door IP-adressen en andere TCP/IP-configuratie-informatie automatisch toe te kennen aan de computers die zijn geïnstalleerd als DHCP-clients.

Door de DHCP-service te installeren kunt u veel van de configuratieproblemen uitbannen die zich voordoen bij het handmatig configureren van TCP/IP.

DHCP is een TCP/IP-standaard voor het vereenvoudigen van beheer van IP-configuratie.

Telkens als een DHCP-client start, vraagt hij aan het DHCP-server om IP-adresseringsinformatie.

Deze adresseringsinformatie bevat het volgende:

- een IP-adres;
- een subnetmasker;
- optionele waarde, zoals het adres van een standaardgateway en van een DNS-server.

Wanneer een DHCP-server een verzoek om een adres ontvangt, selecteert de server IP-adresseringsinformatie uit een groep adressen die is gedefinieerd in zijn database en biedt deze IP-adresseringsinformatie aan aan de DHCP-client.

Als de client het aanbod accepteert, least de DHCP-server de IP-adresseringsinformatie aan de client voor een bepaalde periode.

13.2.1 Het DHCP-leaseproces

De DHCP-service wijst IP-adresseringsinformatie toe aan clientcomputers. De toewijzing van de IP-adresseringsinformatie wordt een DHCP-lease genoemd. Het DHCP-leaseproces, vindt plaats zodra een van de volgende gebeurtenissen zich voordoet:

- TCP/IP wordt voor de eerste maal geïnitialiseerd op een DHCP-client.
- Een client vraagt om een specifiek IP-adres en wordt geweigerd, mogelijk omdat de DHCP-server de lease heeft geannuleerd.
- Een client heeft eerder een IP-adres geleast, maar heeft het IP-adres vrijgegeven en vereist een nieuwe. Een DHCP-lease kan handmatig worden vrijgegeven door ipconfig/release te typen op de opdracht prompt.

13.2.2 De DHCP-service installeren en configureren

Om DHCP te implementeren, moet u de DHCP-service installeren en configureren op ten minste één computer binnen het netwerk waarop Windows 2000 server wordt uitgevoerd. De computer kan worden geconfigureerd als een domeincontroller of een zelfstandige server. Daarnaast moet u, om DHCP goed te laten werken, de TCP/IP-instellingen voor de server handmatig configureren en de clients instellen voor dynamische adresconfiguratie.

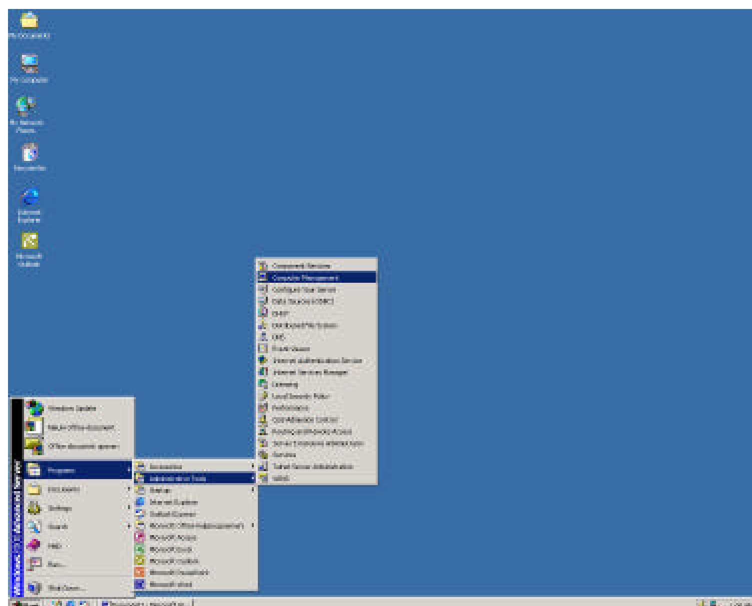
Om de DHCP-service te installeren, gebruikt u het hulpprogramma 'Add/Remove Programs' in het control panel. (De DHCP-service start automatisch tijdens installatie en moet actief zijn om te kunnen communiceren met DHCP-clients.)

Wij raden u aan om als u DHCP in Windows 2000 installeert, helemaal opnieuw te beginnen, aangezien dit een beter resultaat geeft.

Hieronder wordt uitgelegd hoe de installatie wordt uitgevoerd.

- Ga naar 'Start'.
- Ga naar 'Programs'.
- Ga naar 'Administrative Tools'.
- Klik op 'Computer Management'.

Op het scherm zien deze stappen er zo uit:



Figuur 170: Start, Programs, Administrative Tools, Computer Management

Na het starten van 'Computer Management' verschijnt het volgende scherm.



Figuur 171: Windows 2000 Configure Your Server: Networking

- Klik op de optie 'Networking'.

Daaronder verschijnen weer wat andere keuzes, met onder andere DHCP (zie Figuur 171).

- Klik op de optie 'DHCP'.

Het volgende venster verschijnt.

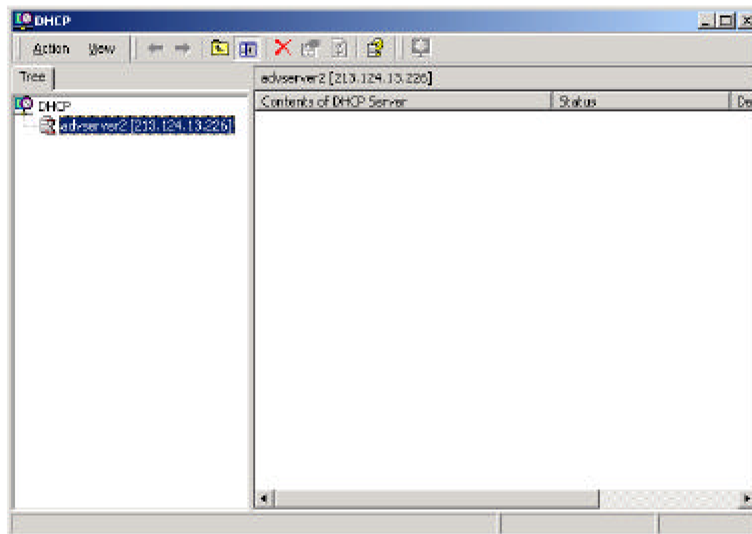


Figuur 172: Windows 2000 Configure Your Server: Networking: DHCP

Dit venster geeft in het kort aan wat handig is te gebruiken bij een DHCP-server.

- Klik op de optie 'Open the DHCP manager'.

Het volgende venster verschijnt.



Figuur 173: DHCP manager

- Selecteer in het tabblad ‘Tree’ (aan de linkerkant) de server ‘adserver2[...]’ en klik met de rechter muisknop.
- Klik op ‘New Scope’.

Het volgende venster verschijnt.



Figuur 174: New Scope Wizard: Welcome

- Klik op de knop ‘Next’.

Het volgende venster verschijnt.

Figuur 175: New Scope Wizard: Scope Name

- Voer achter het veld 'Name' de naam van de computer of de server in.
- Voer achter het veld 'Description' de omschrijving van de bewuste computer/server in.
- Klik op de knop 'Next'.

Het volgende venster verschijnt.

Figuur 176: New Scope Wizard: IP Address Range

- Voer in de velden 'Start IP address' en 'End IP address' het beginadres en het eindadres in van de te maken reeks.

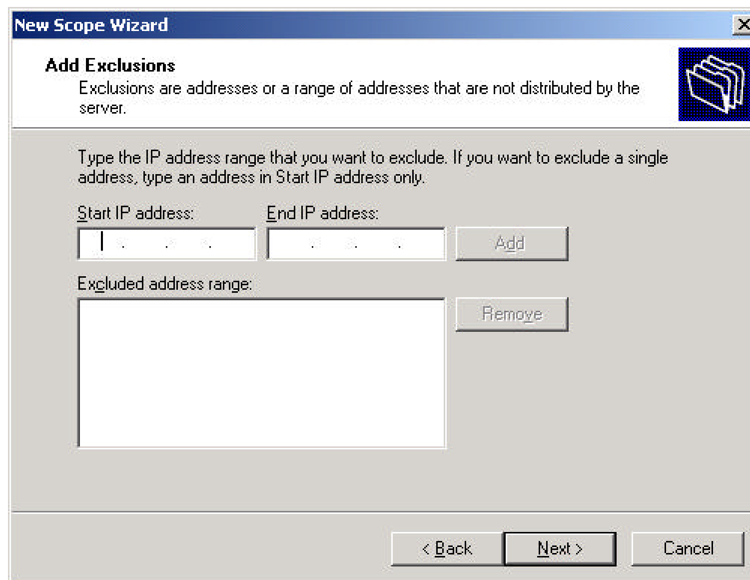
Het veld 'Length' laat u leeg: na het invullen van het subnetmasker wordt dit automatisch ingevuld.

- Voer in het veld 'Subnet mask' het subnetmasker in.

Deze krijgt u samen met de IP-adressen die aan u uitgereikt zijn. In de welkomstbrief staat vermeld welke IP-adressen en subnetmasker van u zijn.

- Klik op de knop 'Next'.

Het volgende venster verschijnt.



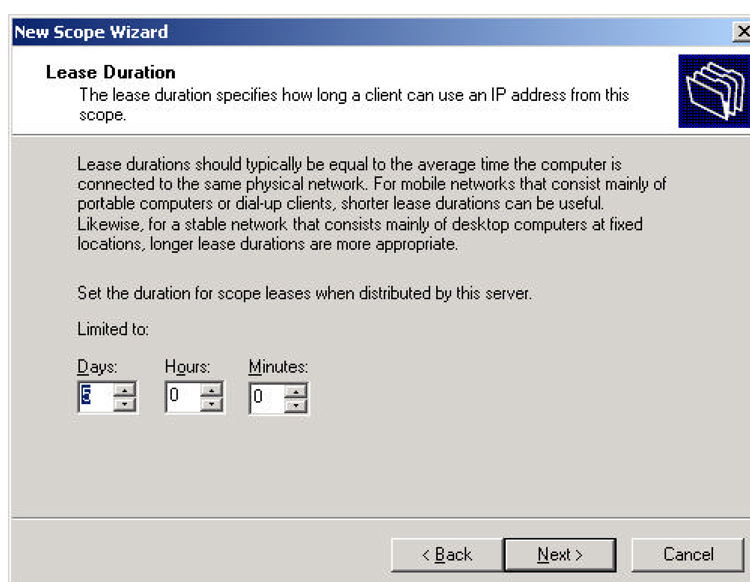
Figuur 177: New Scope Wizard: IP Address Range

- Voer in het selectieblok 'Excluded address range:' eventueel enkele IP-adressen in die u wilt uitsluiten uit de erboven genoemde reeks. Deze IP-adressen kunt u gebruiken voor bijvoorbeeld servers in uw netwerk.

Indien u geen adressen wenst uit te sluiten, gaat u verder:

- Klik op de knop 'Next'.

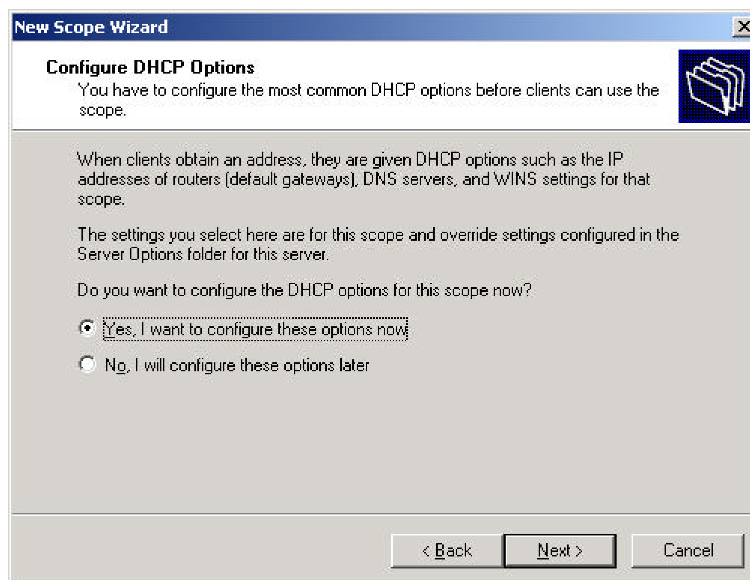
Het volgende venster verschijnt.



Figuur 178: New Scope Wizard: Lease Duration

- Voer onder 'Limited to:' de leasetijd in. U voert dus het aantal dagen, uren en minuten in dat een DHCP-clientlease beschikbaar is vóórdat deze mo et worden vernieuwd.
- Na de tijd te hebben ingesteld, klikt u op de knop 'Next'.

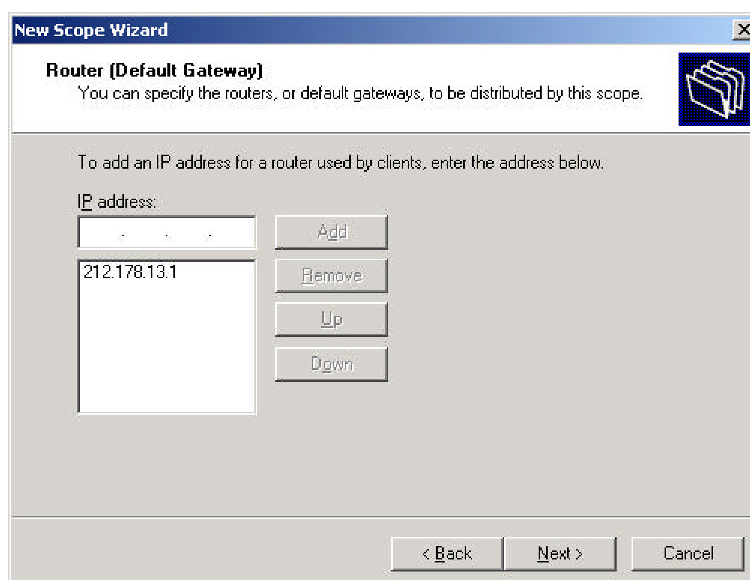
Het volgende venster verschijnt.



Figuur 179: New Scope Wizard: Configure DHCP Options

- Om de scope actief te maken selecteert u het keuzerondje 'Yes, I want to configure these options now'.
- Klik op de knop 'Next'.

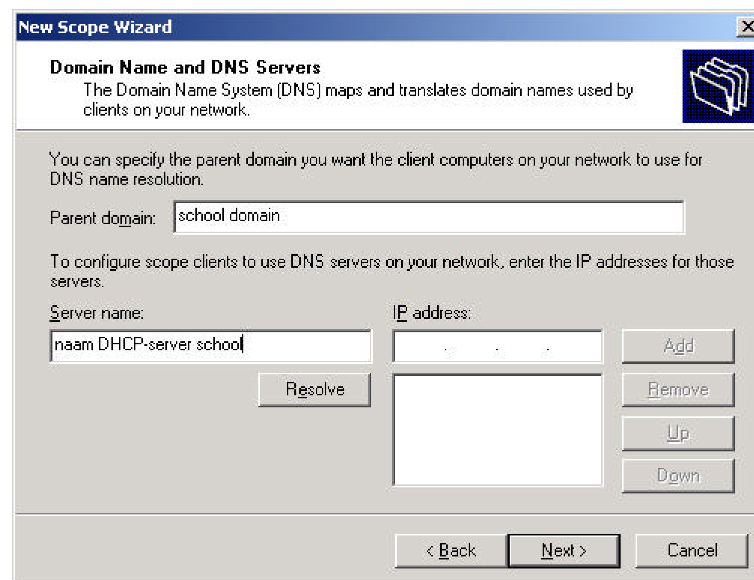
Het volgende venster verschijnt.



Figuur 180: New Scope Wizard: Router (Default Gateway)

- Voer in het veld ‘IP address’ het routernummer in; dit is tegelijkertijd de default gateway van uw organisatie. De DHCP-server weet dan welk nummer voor de router bestemd is.
- Klik op de knop ‘Next’.

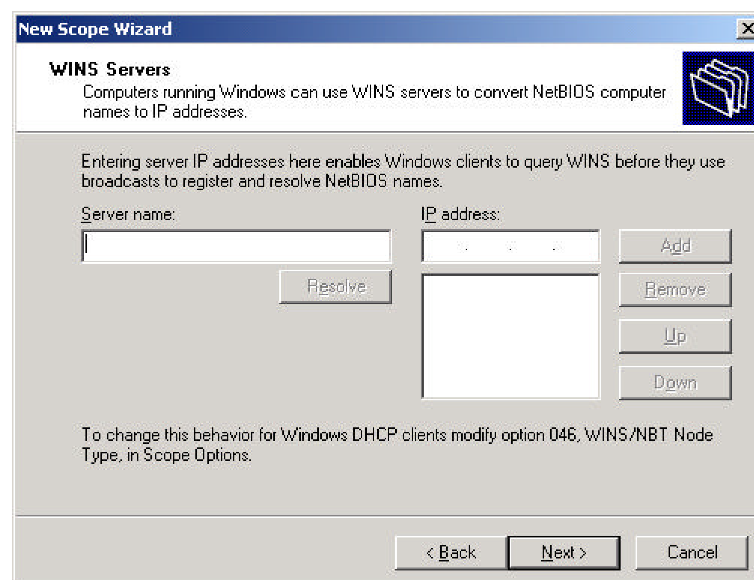
Het volgende venster verschijnt.



Figuur 181: New Scope Wizard: Domain Name and DNS Servers

- Voer in het veld ‘Parent domain:’ de naam van het schooldomein in.
- Voer in het veld ‘Server name’ de naam van de DHCP-server in.
- Klik op de knop ‘Next’.

Het volgende venster verschijnt.

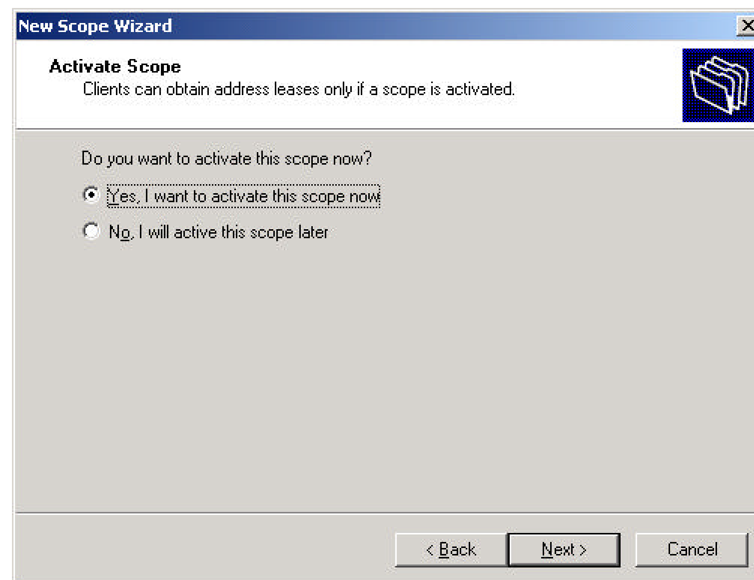


Figuur 182: New Scope Wizard: WINS Servers

Kennisnet ondersteunt geen WINS [14], dus:

- Klik op de knop ‘Next’.

Het volgende venster verschijnt.

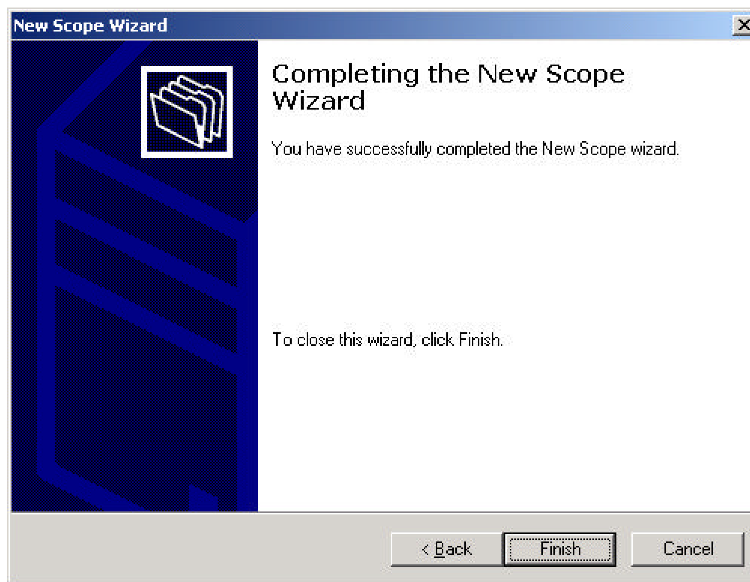


Figuur 183: New Scope Wizard: Activate Scope

- Selecteer het keuzerondje ‘Yes, I want to activate this scope now’.
- Klik op de knop ‘Next’.

Het volgende venster verschijnt.

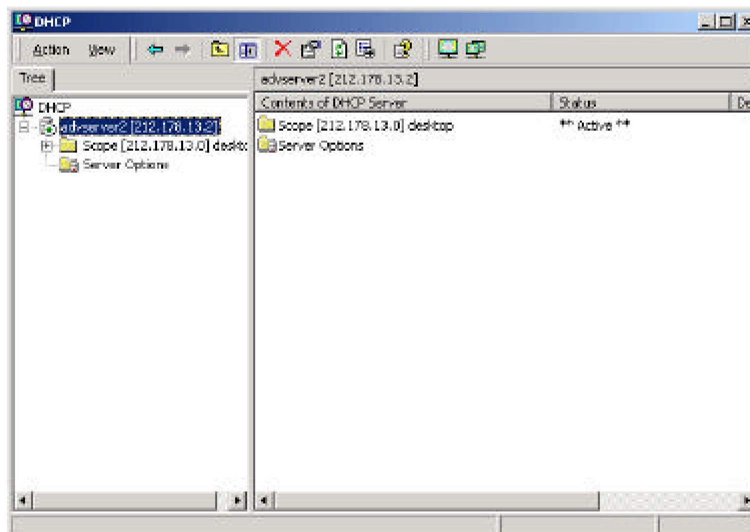
[14] In een gemengde netwerkomgeving gebruiken downloadlevel-clients, zoals computers waarop Windows 98 of Windows 4.0 wordt uitgevoerd, Network Basic Input/Output System (NetBIOS) – namen om te communiceren. Het gevolg is dat een Microsoft Windows 2000 netwerk met downloadlevel-clients een BIOS nodig heeft om namen om te zetten in IP-adressen. WINS is een uitgebreide NetBIOS-naamserver die NetBIOS-computernamen registreert en omzet in IP-adressen. WINS voorziet ook in een dynamische database, die de toewijzing van computernamen naar IP-adressen bijhoudt.



Figuur 184: New Scope Wizard: Completing the New Scope Wizard

- Om de New Scope Wizard te sluiten: klik op de knop 'Finish'.

De scope wordt helemaal geactiveerd, zoals blijkt uit het volgende venster, waarin onder 'Status' te zien is dat de scope geactiveerd is en draait.



Figuur 185: New Scope Wizard: Status van de scope is "Active"

13.3 ISC DHCP-server

De DHCP-server van The Internet Software Consortium (ISC: http://www.isc.org/) kan worden gebruikt op de meest gangbare UNIX-achtige platforms, waaronder:

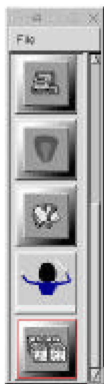
- SunOS/Solaris;
- Mac OS X;
- Linux;
- FreeBSD;
- NetBSD.

Voor een volledige lijst kunt u kijken op de bovengenoemde website van de ISC. Kijk hiervoor bij versie 2; versie 1 is verouderd en versie 3 is nog sterk in ontwikkeling!

Bij RedHat Linux wordt deze DHCP-server in de distributie op CD-ROM meegeleverd en kan ‘on the fly’ worden geïnstalleerd via de Package Manager. Dit gaat zoals hieronder beschreven. Voor andere systemen zult u dit mogelijk ‘met de hand’ moeten doen volgens de instructies in het pakket dat u bij ISC kunt ophalen.

13.3.1 Installatie bij RedHat Linux

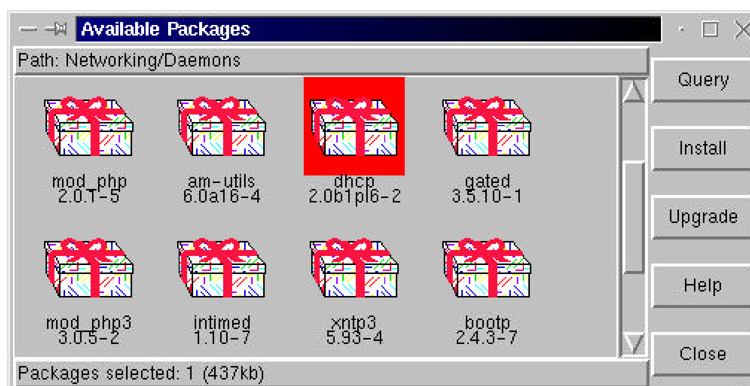
- Open het Control Panel van RedHat Linux (bij een standaardinstallatie start dit voor ‘root’ altijd direct op in een X-sessie).



Figuur 186: RedHat Linux: Control Panel

- Selecteer de ‘Package Manager.
- Klik dan op de knop ‘Available’.

Een volgend venster verschijnt, tenminste wanneer de RPM-bestanden (op de CD-ROM) te vinden zijn. Ga naar ‘Networking’ en dan ‘Daemons’.



Figuur 187: Package Manager, Networking/Daemons, Available Packages

Hier staat, als het goed is, het pakket `dhcp<versie>`.

- Selecteer het pakket.
- Klik op ‘Upgrade’ of ‘Install’ om het te installeren.

De volgende stap is om de DHCP-server te configureren. De service is reeds in de opstartscripts van het systeem verwerkt. Een Reboot is echter niet nodig, zoals zal blijken.

13.3.2 Configuratie

In `/etc/dhcpd.conf` is de configuratie voor de DHCP-server opgenomen. Deze dient u uiteraard aan uw lokale situatie aan te passen. Hieronder is een basisconfiguratie gegeven. De in rood (bij lezen op scherm) of onderstreept (bij lezen op papier) weergegeven teksten dient u (mogelijk) te vervangen voor uw eigen situatie.

```
# dhcpd.conf
#
# Configuratiebestand voor ISC dhcpd
#

# Machines met meerdere netwerkinterface dienen een ‘serveridentificatie’
# (‘server-identifier’) op te geven. Dit dient het primaire IP-adres van
# de machine te zijn, of tenminste een adres dat niet snel zal veranderen
server-identifier 10.1.2.112;
# hier volgen opties voor alle ondersteunde netwerken...
option domain-name “kennisnet.nl”; option domain-name-servers 212.178.5.4,
212.178.5.5;
# Een ‘shared-network’ is bedoeld om netwerkreeksen met dezelfde fysieke #
interface te groeperen. De naam ‘SCHOOL’ is slechts een voorbeeld en # kan
willekeurig worden opgegeven. Gebruik uitsluitend letters en cijfers.
shared-network SCHOOL {
# hier volgen opties voor alle systemen binnen dit ‘shared-network’
  option subnet-mask 255.255.255.128;
  # 1 dag (86400 seconden)
  default-lease-time 86400;
  # 3 dagen
  max-lease-time 259200;

# Deze school heeft slechts één IP-reeks van 128 adressen. Dit wordt
# aangegeven met de opdracht ‘subnet’ en de bijbehorende gegevens.
# Dit is te vergelijken met een ‘Scope’ in de NT-configuratie.
# Opties in dit blok kunnen tussen de accolades (‘{’ en ‘}’) worden
# opgegeven en overschrijven de algemene opties voor het ‘shared-network’
  subnet 10.1.2.0 netmask 255.255.255.128 {
    # Geef met ‘range <begin> <eind>’ aan welke subreeks adressen u
    # wilt uitdelen. Dit kunnen meerdere subreeksen binnen de totale
    # IP-reeks zijn. Dit doet u door meerdere keren de opdracht ‘range’
    # te geven.
    range 10.1.2.3 10.1.2.111;
    option broadcast-address 10.1.2.127;
    option routers 10.1.2.1;
  }
}
```

Figuur 188: Basisconfiguratie DHCP-server

Regels die beginnen met een hekje (#) zijn commentaar. Alle andere regels dienen door een puntkomma (;) te worden afgesloten. Raadpleeg de bij de server behorende documentatie voor meer informatie (UNIX-commando: `man dhcpd.conf`).

Via de webpagina http://enbvlists.kennisnet.nl/techniek/ kunt u, op basis van de aan u uitgedeelde IP-gegevens, een dergelijke DHCP-configuratie laten construeren.

Op de website http://members.xoom.com/vschade/dhcp-conf/ vindt u een hulpmiddel om een DHCP-configuratie te maken en te beheren.

13.3.3 Opstarten

U start de server door het betreffende opstartscript aan te roepen of, indien u de server handmatig hebt geïnstalleerd, door het programma zelf te starten, eventueel met extra parameters.

- Doe bij RedHat Linux:

```
/etc/rc.d/init.d/dhcp start
```

Via de runlevel editor van RedHat Linux (in het ‘Control Panel’) kunt u de DHCP-servers toevoegen aan de gewenste runlevels [15], bijvoorbeeld: 3 tot en met 5.

- Doe ‘Met de hand’:

(Aangenomen is dat de server in de map /usr/sbin is geïnstalleerd; dit kan per systeemimplementatie verschillen.)

```
/usr/sbin/dhcpd
```

[15] Een runlevel is een bepaalde stand van het systeem.

14. Een eigen DNS-server opzetten

Dit hoofdstuk behandelt het opzetten van een eigen DNS-server ten behoeve van het lokale netwerk.

Let op!

Het is belangrijk op te merken dat, wanneer u zelf een DNS-server opzet, u het beste ook een eigen DHCP-server kunt opzetten (zie hoofdstuk 13). U kunt op die manier namelijk aan uw werkstations doorgeven dat deze van uw eigen DNS-server gebruik dienen te maken.

U dient gebruik te maken van de DNS-servers van kennisnet als zogenaamde 'parent' of 'forwarder' (dit zijn twee namen voor hetzelfde). Hoe u dit precies doet, is afhankelijk van het gebruikte product. Veruit het meest gebruikte product is 'BIND' van het 'Internet Software Consortium' (http://www.isc.org/). Veel andere producten zijn gebaseerd op BIND. In de volgende paragrafen wordt voor een aantal producten uitgelegd hoe u deze kunt configureren.

Zoals hierboven al opgemerkt, indien u gebruik wilt maken van uw eigen DNS-server, wordt aangeraden om tevens een eigen DHCP-server op te zetten, waarbij u de correcte IP-adressen voor de DNS-servers opgeeft. Een *andere* optie is om wel gebruik te maken van de centrale DHCP-service, maar in alle systemen uitsluitend de DNS-servers statisch te configureren.

U dient de DNS-server voor uw lokale netwerk in de niet-afgeschermde reeks te plaatsen, zodat deze kan communiceren met de centrale DNS-servers van kennisnet.

14.1 BIND (UNIX)

Voor (vrijwel) elk Unix-achtig besturingssysteem is BIND verkrijgbaar. Bij de meeste Linux-distributies wordt het standaard meegeleverd. Voor installatie: zie ook paragraaf 13.3.1, of de installatiehandleiding van uw besturingssysteem. U kunt ook een broncodedistributie ophalen bij http://www.ics.org/.

Er zijn grofweg twee 'smaken': versie 4.x en versie 8.x. In dit geval wordt uitsluitend versie 8 besproken. Het belangrijkste bestand is '`/etc/named.conf`', dat de basis van de configuratie vormt en aangeeft voor welke 'zones' de nameserver verantwoordelijk is. Alle regels die beginnen met '//' vormen commentaar.

```
// Globale opties voor de DNS-server
options {
        // alle overige bestanden staan in /var/named
        directory "/var/named";
        // gebruikt 'forwarders' voor onbekende gegevens
        forward first;
        forwarders {
          212.178.5.4;
          212.178.5.5;
        };
};

//
// Configuratie voor een 'caching only nameserver'
// (uitgeschakeld)
//zone « . » {
//        type hint;
//        file "named.ca";
//};
```

```
//
// Configuratie voor de 'reverse zone' voor 127.0.0.x
//
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
```

Figuur 189: Basisconfiguratie DNS-server voor UNIX

In de bovenstaande configuratie is de 'caching only'-functie uitgeschakeld. Deze functie zorgt ervoor dat, wanneer onbekend is wat het antwoord op een gestelde vraag is, opgezocht kan worden waar het antwoord wel kan worden verkregen. Hiervoor wordt een lijst met de 'root name servers' (ftp://ftp.rs.internic.net/domain/named.root) gebruikt. Binnen kennisnet heeft het gebruik hiervan geen zin, daar deze servers niet bereikbaar zijn en daarom worden 'forwarders' gebruikt.

Er is echter wel een 'zone' "0.0.127.in-addr.arpa" aangemaakt. Deze zone is noodzakelijk voor het opzoeken van het 'loopback'-adres[16]: 127.0.0.1. Zoals aangegeven in het configuratiebestand is deze zone in het bestand `/var/named/named.local`. Het bestand ziet er als volgt uit:

```
@       IN      SOA     localhost. root.localhost.  (
                              1997022700 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
        IN      NS      localhost.

1       IN      PTR     localhost.
```

Figuur 190: Basisconfiguratie DNS-server voor UNIX: zone voor 'loopback'-adres

Meestal wordt dit bestand, mogelijk met een andere naam, standaard meegeleverd met BIND.

Start BIND en u kunt gebruikmaken van de nameserver. Hoe u BIND precies start, is afhankelijk van uw systeem. U kunt in ieder geval het programma zelf (zonder 'nette' opstartscripts te gebruiken) opstarten met `/usr/sbin/named`. Mogelijk is het pad afwijkend op specifieke systemen; raadpleeg zonodig de bijgevoegde documentatie voor uw systeem.

Onder RedHat Linux kunt u, mits u de standaardinstallatie gebruikt hebt, de service starten met het commando '`/etc/rc.d/init.d/named start`'.

Optioneel kunt u zelf zones toevoegen aan uw configuratie. Voor meer informatie over het opzetten van een DNS kunt u ook de Linux-HOWTO raadplegen:

ftp://metalab.unc.edu/pub/linux/docs/howto/DNS-HOWTO.

14.2 BIND (Windows NT)

BIND voor Windows NT is een afgeleide van de Unix-versie van BIND. Het is gebaseerd op versie 4.9.3. Daardoor is het hoofdconfiguratiebestand anders.

Het configuratiebestand (`named.boot` of `named.ini`) dient u te plaatsen in de Windows-directory (meestal `C:\WINNT`). Alle regels die beginnen met een puntkomma, worden als commentaar beschouwd. Een bestand analoog aan dat voor versie 8.x voor Unix ziet er ongeveer als volgt uit:

[16] De bijbehorende naam is 'localhost'. Dit adres wordt gebruikt om een machine in ieder geval met zichzelf te kunnen laten verbinden. Bijvoorbeeld een commando als 'ping localhost' (Onder Unix, OS/2 of Windows) zal altijd antwoord moeten geven.

```
directory \\var\\named
; cache   .        db.cache

primary 0.0.127.IN-ADDR.ARPA    named.local
forwarders    212.178.5.4 212.178.5.5
```

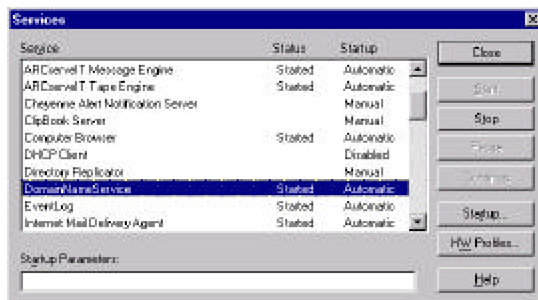
Figuur 191: Basisconfiguratie DNS-server voor Windows NT

De overige bestanden bevinden zich (in dit voorbeeld) in `C:\VAR\NAMED` (onder Windows NT is er geen onderscheid tussen hoofd- en kleine letters). Let op de dubbele 'backslash' (\)! Het bestand 'named.local' is identiek aan dat wat voor de Unix-versie 8.x wordt gebruikt.

U kunt de server starten en stoppen via de 'Services' van Windows NT.

- Open het configuratiescherm.
- Dubbelklik op 'Services'.

Het volgende venster wordt geopend.



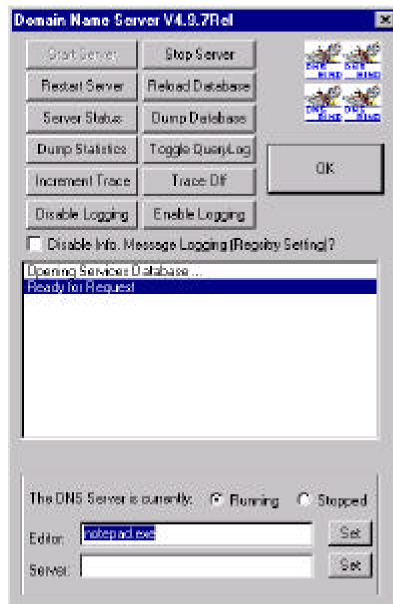
Figuur 192: Windows NT Services: DomainNameService

- Selecteer 'DomainNameService'.
- Met de knoppen 'Start' en 'Stop' kunt u de service bedienen.
- Om de service automatisch te laten opstarten bij het starten van het systeem, klikt u op de knop 'Startup...' (dan wel 'Opstarten') en selecteert u 'Automatic' of 'Automatisch'.

  Let op!

  Zorg ervoor dat er geen andere DNS-server, bijvoorbeeld de Microsoft DNS-Server, actief is wanneer u BIND-NT activeert!

De DNS-service heeft ook een eigen 'Control Panel': de BIND NT DNS Controller, die zich eveneens in het configuratiescherm bevindt.



Figuur 193: BIND-NT Controller, Domain Name Server

- In dit venster kunt u ook de server starten en stoppen, maar ook een actieve server dwingen om de gegevens opnieuw in te lezen (met de knop 'Reload Database').
- Tevens kunt u in dit scherm logbestanden van de DNS-server aan- en uitzetten en bekijken.

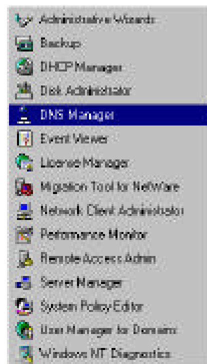
U kunt BIND-NT ophalen op http://www.software.com/scripts/reg-bind.pl. Meer informatie over BIND-NT vindt u op http://www.telemark.net/~randallg/ntdns.htm. Deze web-pagina bevat aanwijzingen over installatie en configuratie van de software.

14.3 Microsoft DNS Server (Windows NT)

Een alternatief voor BIND-NT is de eigen DNS-server van Microsoft, die bij Windows NT-server wordt meegeleverd. De installatie hiervan gaat analoog aan de installatie van de DHCP-server (zie paragraaf 13.1).

Na de herstart van de computer dient de DNS-server te worden geconfigureerd:

- Klik op de Start-knop voor het menu.
- Ga naar de 'Administrative Tools', ofwel de 'Beheerhulpmiddelen'.



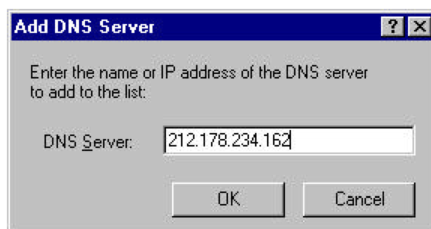
Figuur 194: Administratieve hulpmiddelen

- Open de DNS Manager.

Als het de eerste keer is dat u de DNS Manager opstart, staat er uitsluitend een icoontje van de 'Server List'.

- Klik met de rechter muisknop op de 'Server List' en kies 'Add DNS Server' (of het equivalent in het Nederlands).

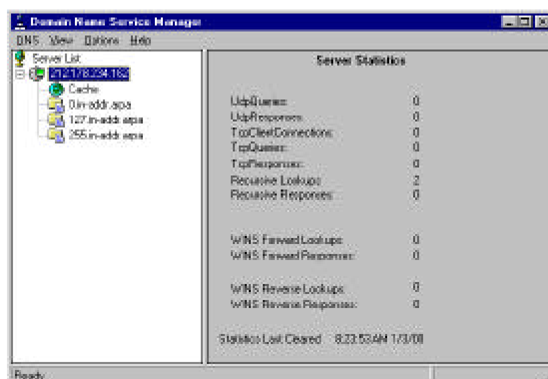
Het volgende venster verschijnt.



Figuur 195: Add DNS-server

- Voer het IP-adres in of de DNS-naam van de server die u toe wilt voegen.
- Klik vervolgens op de knop 'OK'.

Er wordt een server-icoontje aangemaakt.



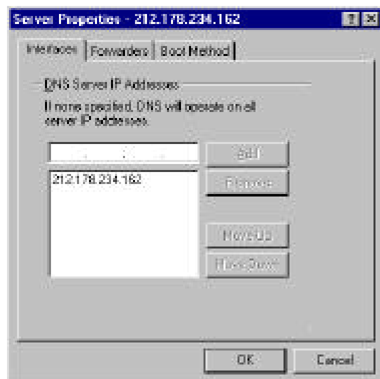
Figuur 196: Domain Name Service Manager

- Dubbelklik op het icoontje om het uit te vouwen.

Er verschijnt een lijstje met de 'Cache' en een aantal voorgedefinieerde zones.

- Klik nu met de rechter muisknop op de zojuist aangemaakte server.
- Kies 'Properties' (of 'Eigenschappen').

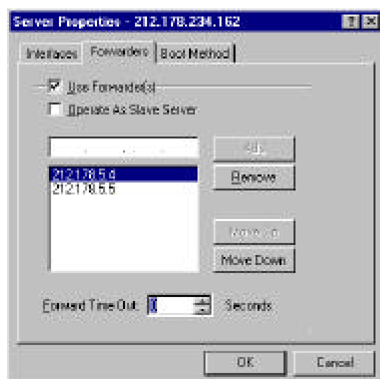
Er verschijnt een klein venster met een drietal tabbladen.



Figuur 197: MS DNS Server, Server Properties, Interfaces

Op het tabblad 'Interfaces' (zie Figuur 197) kunt u aangeven op welke interfaces de DNS-server moet 'luisteren'. Dit zijn de IP-adressen van de netwerkkaarten, indien er meerdere zijn. Meestal zult u de standaardinstellingen kunnen gebruiken.

Het tweede tabblad is 'Forwarders'.



Figuur 198: MS DNS Server, Server Properties, Forwarders

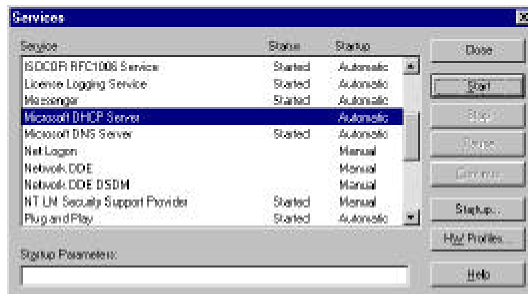
Op het tabblad 'Forwarders' kunt u de IP-adressen van de 'forwarding DNS-servers', in dit geval de centrale DNS-servers van kennisnet, aangeven.

- Selecteer het aanvinkvakje 'Use Forwarder(s)' en voer de IP-adressen (212.178.5.4 en 212.178.5.5) in.
- U kunt ervoor kiezen om ook het aanvinkvakje 'Operate As Slave Server' te selecteren. Dit zorgt ervoor dat *alle* verzoeken worden doorgestuurd en er niet naar lokale zones/domeinen wordt gekeken.
- Open het configuratiescherm voor de 'Services' met de volgende knop:



Figuur 199: Windows NT Services

Het volgende venster verschijnt.



Figuur 200: Configuratiescherm Services

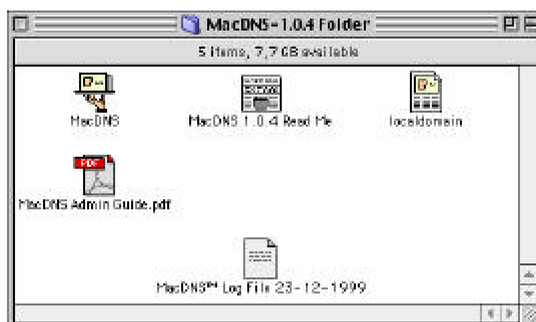
- Selecteer de 'Microsoft DNS Server'.
- Controleer de 'Status'. Indien de status 'Started' is, is de service reeds actief. Anders dient u deze alsnog te starten met 'Start', rechts in het venster.
- Controleer de 'Startup'.De vermelding onder 'Startup' dient "Automatic"/ "Automatisch" te luiden. Dit kunt u eventueel aanpassen met de knop 'Startup...'.

14.4 MacDNS

Voor de Apple Macintosh kunt u MacDNS gebruiken om een eigen DNS-server op te zetten. MacDNS is helaas niet zo uitgebreid als BIND of de Microsoft DNS-server, maar is redelijk eenvoudig te bedienen. Volg bij het installeren de aanwijzingen die in het begeleidende tekstbestand staan ('MacDNS <*versie*> Read Me'). Zo dient u een 'alias' van het programma in de opstartmap te plaatsen om MacDNS automatisch te starten bij het opstarten van het systeem.

Om MacDNS te configureren, gaat u als volgt te werk.

- Open de opstartmap.



Figuur 201: Map MacDNS

- Start 'MacDNS'.

U krijgt, als het goed is, het venster met de logs te zien:

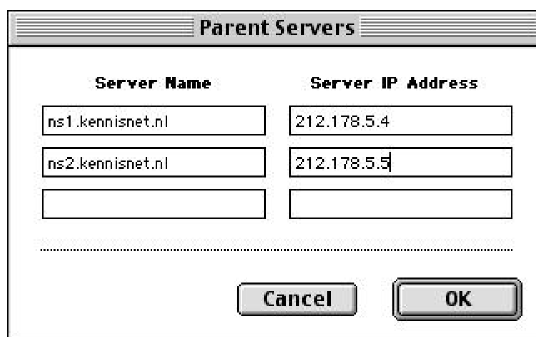


Figuur 202: MacDNS: Message Log

Hier staan alle wijzigingen die u uitvoert, informatie over gebeurtenissen, foutmeldingen, enzovoort.

- Kies uit het menu ‘Hosts’ de optie ‘Set Parent Servers’.

Het volgende scherm verschijnt.



Figuur 203: MacDNS: Parent Servers

U kunt een maximum van drie ‘parents’ opgeven.

- Links dient u de naam van de server in te voeren en rechts het bijbehorende IP-adres. Voor kennisnet voert u in:

  ‘`ns1.kennisnet.nl`’ met adres `212.178.5.4`

  ‘`ns2.kennisnet.nl`’ met adres `212.178.5.5`.

Wanneer u geen eigen domein wilt aanmaken, bent u nu in principe klaar.

Om zelf een domein toe te voegen, doet u het volgende:

- Toets het Command-N (‘Appeltje -N’) in.

Het ‘Zone Information’-scherm verschijnt.

Figuur 204: MacDNS: Zone Information

- U kunt hier de domeinnaam, de eerste en eventueel de tweede nameserver en het mailadres van de beheerder ('Administrator') invoeren.

Tevens kunt u enkele periodes opgeven:

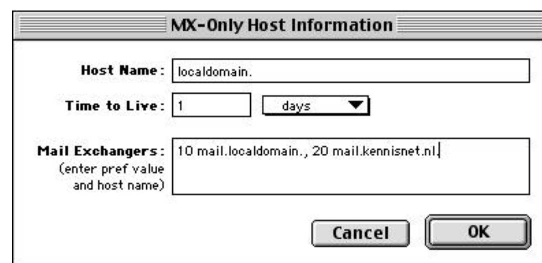
- **Refresh Interval:** de tijd die moet verstrijken voordat een 'secondary' (kopie) nameserver controleert of er weer nieuwe informatie over de zone beschikbaar is.
- **Retry Interval:** de tijd die verstrijkt voordat de secondary nameserver, na een mislukte poging de zone over te halen, dit opnieuw probeert.
- **Expire Interval:** de tijd waarna een secondary nameserver de opgeslagen gegevens *moet* verwijderen.
- **Minimum TTL:** de periode waarin gegevens over een host opgeslagen mogen worden in de buffers van een andere DNS-server.

Met het scherm 'Host Information' (Command-H) kunt u een host toevoegen.

Figuur 205: MacDNS: Host Information

- U dient ten minste de betreffende nameserver toe te voegen. De naam die u achter 'Host Name' invoert, dient ten minste de domeinnaam te bevatten.
- Het IP-adres is verplicht om in te voeren.
- De 'Time to Live' is hetzelfde als 'Minimum TTL' voor een zone, maar dan specifiek voor één machine.
- Achter 'Aliases:' kunt u, door komma's gescheiden, eventuele aanvullende namen voor dezelfde machine opgeven.
- Achter 'Mail Exchangers:' voert u, eveneens door komma's gescheiden, een prioriteit (getal) en een volledige machinenaam (eindigend met een punt!) voor de mailserver voor deze machine in. De prioriteit is een numerieke waarde: hoe lager het getal, hoe hoger de prioriteit, ofwel hoe eerder deze benaderd zal worden om de mail te bezorgen.

Het is ook mogelijk om alleen een 'Mail Exchanger' voor een (sub)domein op te geven, zonder dat er een IP-adres aan wordt gekoppeld.



Figuur 206: MacDNS: MX-Only Host Information

- Om voor de zone zelf een 'Mail Exchanger' aan te geven, dient u geen machinenaam op te geven bij 'Host Name:', maar uitsluitend het domein!
- Achter 'Mail Exchangers:' vult u de prioriteiten en de volledige namen van de mailservers in.

15. De eigen proxy-server blijven gebruiken

U kunt de eigen webproxy blijven gebruiken, mits deze ondersteuning biedt voor het Internet Caching Protocol (ICP) of Caching Array Routing Protocol (CARP) voor web. Met één van deze protocollen kan uw eigen webproxy als 'slave' van de proxy-server in het serverpark fungeren.

15.1 De eigen proxy-server aan de proxy-server van kennisnet koppelen

Daarvoor dient u de proxy-server zo te configureren dat deze op zijn beurt gebruikmaakt van de proxy-server in het serverpark (proxy.kennisnet.nl) via ICP of via CARP. Hoe dit precies werkt is afhankelijk van de gebruikte software.

- Open het configuratiescherm van uw proxy-server en geef de kennisnetproxies op als 'ouder' ('parent') van uw proxy. Voor ICP dient u poort 3130 van `proxy.kennisnet.nl` op te geven; voor CARP dient u poort 8080 van `proxy.kennisnet.nl` op te geven.

Meer informatie kunt u (onder meer) vinden op de volgende adressen:

- http://www.microsoft.com/proxy/documents/CarpWP.exe
- http://cgi.netscape.com/proxy/v3.5/index.html
- http://developer.netscape.com/docs/manuals/proxy.html
- http://www.csm-usa.com/proxy/admin/carp/
- http://cache.is.co.za/squid/

15.2 CSM Proxy

Voor de CSM-proxy is een redelijk uitgebreid, Engelstalig handboek te vinden, op de website van CSM. Op het onderstaande adres vindt u de uitleg over het instellen van CARP:

http://www.csm-usa.com/proxy/admin/carp/.

U dient als 'parent' "`proxy.kennisnet.nl`", of apart "`proxy1.kennisnet.nl`" én "`proxy2.kennisnet.nl`" op te geven.

15.3 Netscape Proxy

Netscape heeft een grote verzameling on line handboeken van de verschillende producten. Hier kunt u de handleidingen vinden voor zowel de Windows NT-versie als de UNIX-versie van de Netscape Proxy. Het adres voor de proxy-handleidingen is:

http://developer.netscape.com/docs/manuals/proxy.html.

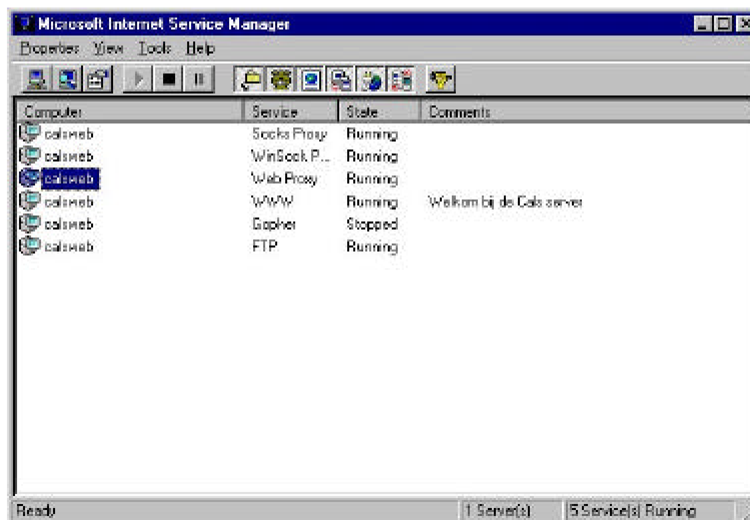
15.4 Microsoft Proxy[17]

Het is mogelijk om met de Microsoft Proxy (voor Windows NT) een relatie met de centrale kennisnet-proxies te definiëren en zo uw eigen netwerk lokaal proxy-functionaliteit te bieden. Hiertoe dient u als volgt te werk te gaan:

- Start de Internet Service Manager.

Het volgende scherm verschijnt.

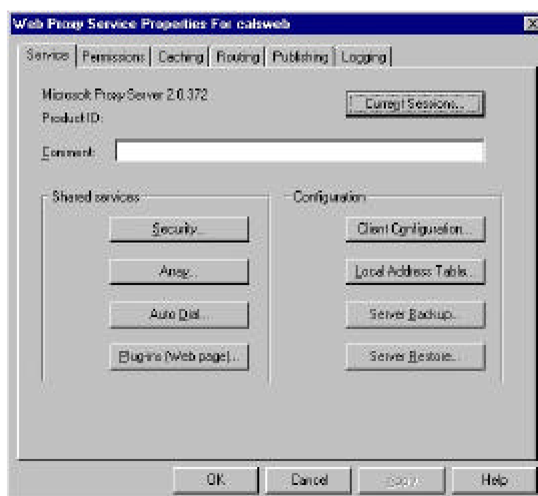
[17] Met dank aan Harry Spek, ICT-coördinator Calscollege Nieuwegein.



Figuur 207: Microsoft Internet Service Manager

- Verifieer dat de webproxy actief is. Indien dat het geval is, staat in de kolom ‘State’ de vermelding “Running”.
- Dubbelklik vervolgens op de computernaam helemaal links om de instellingen voor de dienst aan te passen.

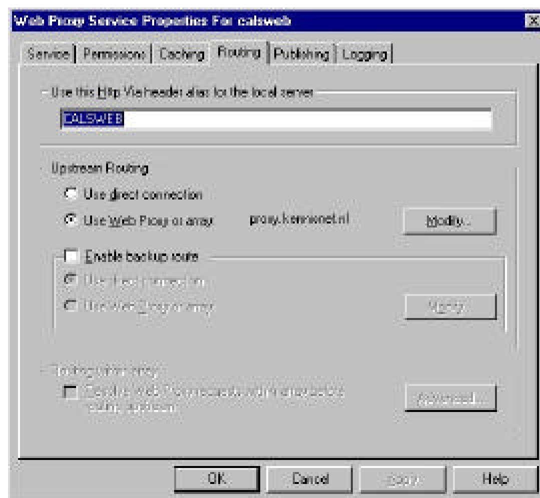
Een venster met tab-bladen verschijnt.



Figuur 208: Web Proxy Service Properties, Service

- Op het tabblad ‘Service’ (zie Figuur 208) kunt u enkele zaken instellen, waaronder een omschrijving van de dienst achter ‘Comment:’. Deze opties dient u naar eigen inzicht en behoefte in te vullen; raadpleeg hiervoor uw handleiding van de Microsoft Proxy.

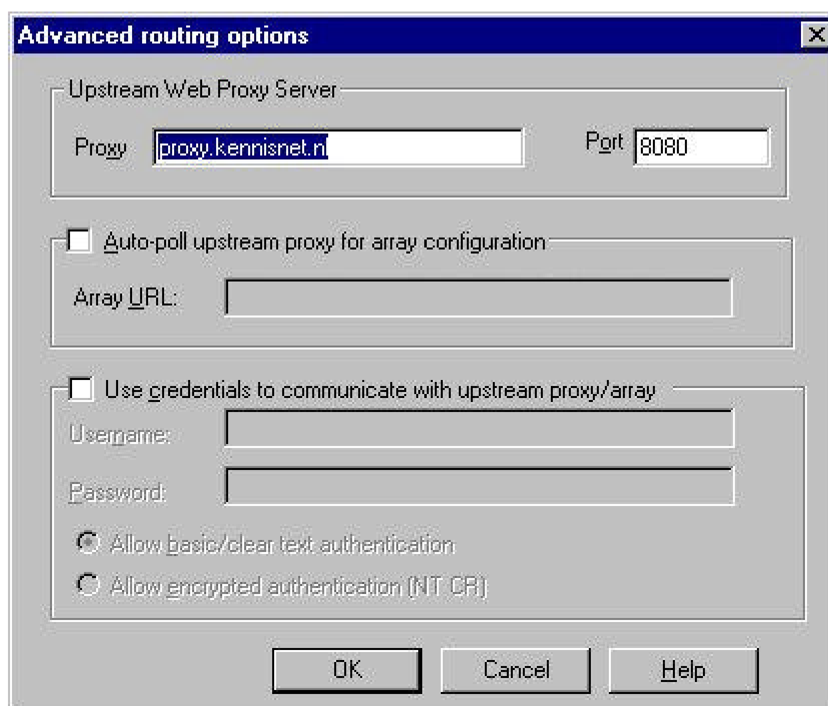
Een ander tabblad is ‘Routing’.



Figuur 209: Web Proxy Service Properties, Routing

- Op het tabblad ‘Routing’ (zie Figuur 209) dient u in het invoerveld de machinenaam in te voeren, ofwel de naam waarnaar verwezen kan worden als zijnde de proxy-server. Het is bij het instellen van de bladerprogramma’s van belang om te weten dat u daarvoor de Microsoft Proxy-poort 80 (en niet poort 8080!) dient te gebruiken.
- In het vakje ‘Upstream Routing’ dient u de optie ‘Use Web Proxy or array’ te selecteren.
- Klik vervolgens op de knop ‘Modify...’ om de instellingen aan te passen.

Het volgende venster verschijnt.



Figuur 210: Advanced routing options

- Voer achter het veld ‘Proxy’ in: “proxy.kennisnet.nl”.

- Voer poortnummer “8080’”in achter het veld ‘Port’.
- Laat de andere opties op het tabblad **uit**geschakeld.
- Klik op de knop ‘OK’ om het venster te sluiten.
- Sluit de opties voor de proxy -server om terug te keren naar ‘Internet Service Manager’.

16. De eigen lokale mailserver blijven gebruiken

U kunt de eigen lokale mailserver van de organisatie blijven gebruiken. U dient hiervoor een verzoek in te dienen bij het Servicepunt Kennisnet op het adres: http://servicepunt.kennisnet.nl/.

U dient een eigen domeinnaam aan te vragen, voorzover u hierover nog niet beschikt. Hierin kan door kennisnet, als Internet Service Provider, worden voorzien. Alle e-mail voor uw eigen domein zal worden doorgestuurd naar uw eigen mailserver. U dient uw lokale mailserver zo in te stellen, dat deze de mailservers van kennisnet (`smtp.kennisnet.nl`) als *smart host* of als *mailrelay* gebruikt voor uitgaande mail.

Let op!

Er is nog niet voorzien in een mogelijkheid om uw mail weer van buiten kennisnet op te halen vanaf uw lokale mailserver. Technisch gezien is het wel mogelijk, maar dit vereist toestemming van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het zal nader moeten worden bepaald of, en zo ja, hoe in deze mogelijkheid zal worden voorzien.

Om u enigszins op weg te helpen wordt van mailsystemen waarvan deze informatie bekend is, in de volgende paragrafen beschreven hoe deze kunnen worden ingesteld voor gebruik op kennisnet.

16.1 Sendmail

Veruit het meest gebruikte mailsysteem op het internet is Sendmail. Sendmail is beschikbaar voor vrijwel iedere UNIX-variant en OS/2. Om Sendmail zodanig te configureren dat de mailservers van kennisnet als ‘smart host’ gebruikt worden, dient u het configuratiebestand aan te passen. Over het algemeen is de configuratie van Sendmail bepaald niet eenvoudig, maar deze handeling is relatief eenvoudig.

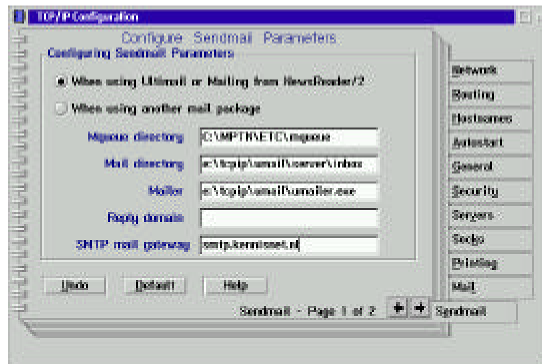
Voor UNIX-varianten zijn de instructies als volgt:

- Open het bestand ‘`/etc/sendmail.cf`’ in uw favoriete tekst-editor en zoek naar de letters “DS” aan het begin van de regel. Eventueel kunt u ook zoeken naar het woord “relay”, daar de optie veelal door een commentaarregel wordt voorafgegaan. Voor OS/2 dient u gebruik te maken van de beheerinterface bij de TCP/IP-configuratie
- Direct achter “DS”, dus zonder spatie, voert u de naam van de mailservers van kennisnet in, namelijk “`smtp.kennisnet.nl`”. Hieronder volgt een fragment uit een configuratiebestand:

```
# “Smart” relay host (may be null)
DS
```

Figuur 211: Unix : Sendmail-configuratie (fragment)

- Voor OS/2 Sendmail opent u het configuratievenster voor TCP/IP (LAN).
- Ga naar het tabblad ‘Sendmail’.



Figuur 212: OS/2, TCP/IP Configuration, Sendmail (pag. 1)

Dit tabblad bestaat uit twee pagina's, maar alleen de eerste is nu van belang.

- Voer in het onderste veld, 'SMTP mail gateway', de naam van de mailservers van kennisnet in: "`smtp.kennisnet.nl`".
- Indien nodig kunt u Sendmail zo instellen, dat het bij een herstart van het systeem automatisch wordt opgestart. Hiervoor dient u op het tabblad 'Autostart' de optie 'Autostart service' voor Sendmail in te schakelen.

Meer informatie over Sendmail en de configuratie hiervan kunt u vinden op de website van Sendmail: http://www.sendmail.org/.

16.2 E-mail vanaf internet lezen zonder POP of IMAP

Als de e-mail niet kan worden gelezen omdat de eigen webserver vanaf internet niet met POP of IMAP te bereiken is, moet u iets extra's doen om dit toch te bewerkstelligen.

Bij sommige mailservers zit de mogelijkheid om een webmailserver aan uw eigen mailserver te koppelen. Soms is deze functie zelfs geïntegreerd in het systeem. Ook bestaan er softwarepakketten om een eigen webmailserver op te zetten en deze via bijvoorbeeld IMAP uw 'normale' mailserver te laten raadplegen.

Kortweg: via een webinterface kunt u uw e-mail beschikbaar maken. Behalve het opzetten van een webmailserver dient u een verzoek in te dienen voor 'reverse proxy' (zie paragraaf 17.2).

17. Een eigen webserver opzetten

17.1 Een eigen webserver of een plek in het Kennisnet Webhotel

U bent uiteraard helemaal vrij in de keuze om een eigen webserver in te richten of gebruik te maken van het Kennisnet Webhotel (zie deel IV) om uw website aan de buitenwereld aan te bieden. Beide opties hebben zo hun voor- en nadelen. Zo heeft een eigen webserver het grote voordeel dat u alle vrijheid hebt om te doen en te laten wat u wilt met de inhoud en scripting, de hoeveelheid schijfruimte enzovoort. Uw eigen website staat bovendien dicht bij uw eigen gebruikers (leerlingen en docenten).

Aan de andere kant dient u voor dit doel wel over een machine te beschikken met voldoende capaciteit en zult u – als u uw website wilt publiceren op kennisnet – moeten overwegen meer bandbreedte in te kopen voor uw aansluiting op kennisnet. U moet bovendien de machine zelf beheren, terwijl dat voor u wordt gedaan in het geval van het webhotel.

Indien u uw eigen webserver op het internet 'zichtbaar' wilt maken, moet u via het Servicepunt Kennisnet een verzoek voor een 'reverse proxy' indienen op het adres: http://servicepunt.kennisnet.nl/.

17.2 De werking van een 'reverse proxy'

Om uit te leggen wat een 'reverse proxy' is en wat deze doet, dient u iets te weten over het HTTP-protocol. Wat u bijvoorbeeld nooit ziet, is wat uw internet-browser (bladerprogramma voor internet, zie deel III) werkelijk doet wanneer er een bestand of web-pagina wordt opgevraagd. Het simpelst mogelijke verzoek om bijvoorbeeld de hoofdpagina van een webserver te krijgen, is het volgende:

```
GET / HTTP/1.0
```

Het verzoek begint met een commando. In dit geval wordt 'GET' gebruikt, maar er zijn meer commando's, doch deze zijn op dit punt niet zo relevant. Na een spatie volgt het gevraagde object (in dit geval de hoofdpagina, aangeduid met '/') en na nogmaals een spatie 'HTTP', een schuine streep ('/') en het versienummer van het protocol.

Na deze regel zouden nog enkele opties kunnen volgen van de vorm 'Optie: waarde'. In een dergelijke optieregel kan het bladerprogramma zich voorstellen aan de webserver, vertellen welke taal u prefereert, enzovoort. Na alle opties volgt een lege regel, waarna de webserver zal antwoorden.

Op dit moment is versie 1.1 de meest gangbare versie van het HTTP-protocol. In HTTP/1.1 is er één vereiste optie, namelijk 'Host:'. Na 'Host:' wordt het adres van de website (bijvoorbeeld www.kennisnet.nl) gegeven. Deze optie bepaalt welke gegevens de webserver zal retourneren:

```
GET / HTTP/1.1
Host: www.kennisnet.nl
```

Op basis van deze naam zullen de gegevens uit een bepaalde map worden opgehaald.

De reverse proxy werkt eigenlijk op dezelfde manier, maar niet met lokale mappen. De reverse proxy heeft een tabel met de host-namen van websites binnen kennisnet, waarvoor een reverse proxy is ingericht. Naast de host-namen zijn de IP-adressen of echte namen van de webservers vermeld. Wanneer een verzoek binnenkomt voor bijvoorbeeld www.school.nl, dan wordt het bijbehorende adres gezocht voor de echte webserver en maakt de reverse proxy-server een verbinding met deze machine. Het binnengekomen verzoek wordt 1-op-1 doorgestuurd en het antwoord wordt weer netjes teruggegeven aan de verzoekende internet-browser.

Wanneer u uw eigen webserver op het internet beschikbaar wilt laten maken, wordt er een extra regeltje aan de tabel toegevoegd.

17.3 De basis voor een eigen webserver

De eerste vraag die u zich moet stellen, is wat u precies wilt gaan doen met uw website en welke middelen u nodig denkt te hebben. Op welk computerplatform wilt u uw website opzetten? Als u dat weet, kunt u bepalen welke webserver u gaat gebruiken.

Voor een aantal webservers zal in de volgende paragrafen worden uitgelegd hoe u deze kunt opzetten.

17.4 Apache

Apache is veruit de meest gebruikte webserver. Apache is gratis en voor zeer veel besturingssystemen (vooral UNIX-achtige, maar ook OS/2 en Windows NT) beschikbaar. Via http://www.apache.org/ kunt u aan de meest recente versie van Apache komen, vaak al voorgecompileerd (lees: kant-en-klaar) voor uw besturingssysteem.

Bij de meeste Linux-distributies is de installatie van Apache niet veel meer dan het installeren van het juiste pakketje. Daarna kunt u 'met de hand' het proces starten of zal de webservice bij het opstarten van Linux automatisch worden gestart.

Nu moet u Apache nog aan uw eigen situatie aanpassen. Het is belangrijk om te weten waar Apache is geïnstalleerd op uw systeem. De standaardlocatie verschilt vrij sterk tussen verschillende distributies en besturingssystemen. De installatie van Apache vindt u bij de volgende systemen in de erbij vermelde mappen:

Systeem	Wat?	Mappen

Systeem	Wat?	Mappen
RedHat Linux en Linux PPC	configuratie	`/etc/httpd/conf`
	logbestanden	`/etc/httpd/logs`
	webpagina's	`/home/httpd/html`
	CGI-programma's	`/home/httpd/cgi-bin`
Slackware Linux	configuratie	`/var/lib/httpd/conf`
	logbestanden	`/var/lib/httpd/logs`
	webpagina's	`/var/lib/httpd/docs`
	CGI-programma's	`/var/lib/httpd/cgi-bin`

Over het algemeen zal uw webserver zonder aanpassingen kunnen functioneren, maar het is niet onverstandig om de configuratiebestanden te controleren en eventueel opties bij te werken. Hoogstwaarschijnlijk treft u de volgende bestanden aan in de configuratiemap:

- **`httpd.conf`** Dit bestand bevat de basisconfiguratiegegevens, zoals het aantal subprocessen dat gestart moet worden, te reserveren capaciteit, enzovoort.
- **`access.conf`** Dit bestand bevat informatie over door wie en vanaf waar bepaalde gegevens mogen worden bekeken.
- **`srm.conf`** In dit bestand worden overige opties, zoals aanvullende bestandsassociaties, koppelingen van typen bestanden aan benamingen en icoontjes gedefinieerd.
- **`mime.types`** Dit bestand bevat een lijst van zogenaamde MIME-types (gestandaardiseerde aanduidingen voor bestandsformaten), gekoppeld aan de bestandsnaam-extensie (`.txt`, `.html`, `.gif` en dergelijke).

De trend is thans om alle configuratieopties weer, zoals dat een paar jaar geleden gebruikelijk was, onder te brengen in alleen '`httpd.conf`'. In alle genoemde bestanden is bij de opties reeds voorzien in beknopte uitleg van de functie. Meer informatie kunt u echter vinden op http://www.apache.org/, onder 'Documentation'.

Wanneer de configuratie naar uw zin is, herstart u de webserver (alleen het proces, niet de hele computer!). Dit doet u vaak vanuit de root met een commando zoals één van onderstaande:

- `/etc/rc.d/init.d/httpd restart` (RedHat/LinuxPPC)
- `/etc/rc.d/httpd restart` (SuSe)
- `/etc/init.d/httpd restart` (Solaris)
- `kill -HUP 'cat /var/lib/httpd/logs/httpd.pid'` (Slackware)

U kunt nu uw webpagina's plaatsen in de juiste map. Zorg wel dat het webserverproces de bestanden kan lezen (voer het commando '`man chmod`' uit voor meer informatie op een UNIX-systeem). Door nu met een internet-browser uw website te benaderen, kunt u bekijken of het er uitziet zoals u dat in gedachten had.

17.5 Mac OS Persoonlijke webserver

Bij de meer recente versies van Mac OS zit standaard een 'Persoonlijke webserver'. Hiermee kunt u zeer eenvoudig een eigen webserver opzetten. U hoeft de webserver eigenlijk alleen maar in te schakelen. Zorg wel dat uw TCP/IP-instellingen correct zijn!

Controleer allereerst of op uw systeem de 'webserver-extensie' is ingeschakeld.

- Open het regelpaneel 'Extensiebeheer' (Control Panel: 'Extensions').

Het regelpaneel verschijnt.


Figuur 213: Extensiebeheer

- Zoek in de lijst de ‘Webserver-extensie’ op. Als er een kruisje voor deze extensie staat, is deze reeds actief.

  Indien dat niet het geval is, klik dan op het vierkantje om de extensie in te schakelen en klik vervolgens op de knop ‘Herstart’.

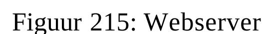
Na een eventuele herstart kunt u de webserver activeren via de regelbalk.

Op de regelbalk, die zich normaliter onder aan uw beeld bevindt, staat een klein icoontje, waar een menu bij hoort.


Figuur 214: Regelbalk: Persoonlijke webserver

Via het menu dat dan verschijnt, kunt u de webserver aan- en uitschakelen (‘Schakel webserver in’).

Wanneer u nog zaken wilt instellen, dan kunt u dat via het regelpaneel ‘Webserver’ doen. Open, via de regelbalk of via het Apple-menu, deze regelbalk om het volgende venster te openen:


Figuur 215: Webserver

Standaard is de locatie waar uw webpagina's zich bevinden '`<disknaam>:Webpagina's`' (voor anderstalige versies van Mac OS zal dit afwijken).

- Dit kunt u met de bovenste 'Selecteer...'-knop aanpassen.
- De onderste 'Selecteer...'-knop kunt u benutten om een specifieke naam te gebruiken voor de openingspagina van een map. Selecteer bijvoorbeeld 'Standaard.html'.

U kunt in dit regelpaneel ook de webserver stoppen en starten. Bovendien bestaat hier de mogelijkheid om mensen toegang te geven tot de bestanden op basis van Samengebruik-profielen. Het wordt *niet* aangeraden om dit in te schakelen, tenzij u *echt* weet wat u doet!

Als alles is ingeschakeld en geconfigureerd, kunt u de website benaderen via het adres van uw Mac-server. Wanneer u uw webserver hebt gestart, zijn de mogelijke adressen ook te zien in het regelpaneel 'Webserver' bij 'Mijn adres'.



Figuur 216: Mac OS Persoonlijk webserver

De 'Mac OS Persoonlijke webserver' biedt geen bijzondere mogelijkheden, maar is voor een eigen webserver een snelle en eenvoudige oplossing.

17.6 CGI en de werking ervan

CGI is de afkorting voor 'Common Gateway Interface'. CGI zorgt ervoor dat er op basis van gebruikersinvoer dynamisch webpagina's kunnen worden gegenereerd. Als u bijvoorbeeld een formulier op een webpagina invult en dan op de verzendknop klikt, wordt er informatie van uw internet-browser (bladerprogramma voor internet, zie deel III) naar de webserver verstuurd. Dit kan grofweg op twee manier. Het HTTP-protocol kent hiervoor het GET-commando en het POST-commando.

In het geval van het GET-commando wordt er een verlengd adres gegenereerd. Uw internet-browser krijgt bijvoorbeeld de instructie om bij het klikken op de verzendknop het adres http://www.school.nl/cgi-bin/formulier.pl op te roepen. Achter dit adres wordt vervolgens een vraagteken geplaatst en een lijst van parameters met waarden, gescheiden door een ampersand (&):
`?parameter1=waarde&parameter2=waarde2`

Dit resulteert dan in een volledig adres als:

http://www.school.nl/cgi-bin/formulier.pl?a=jan&b=jansen

De parameters en waarden worden overigens wel op een dusdanig manier gecodeerd dat speciale tekens in de parameternamen en in de waarden netjes worden geïnterpreteerd. Speciale tekens zijn onder meer het ampersandteken (&), spaties, plusteken (+), is-teken (=).

Het deel achter het vraagteken wordt door middel van een variabele aan een programma op de server doorgegeven. Dit programma kan de gegevens decoderen en opsplitsen. Op basis van de gegevens zal het bepaalde acties uitvoeren en een nieuwe webpagina, een afbeelding, tekst of iets dergelijks genereren.

Het verschil met het POST-commando is tweeledig. Enerzijds is de overdracht van informatie van de internet-browser naar de webserver anders, anderzijds is de manier waarop het betreffende programma op de webserver de informatie aangeleverd krijgt, anders.

Het adres dat de internet-browser krijgt, wordt ongemoeid gelaten. In plaats daarvan wordt de informatie niet in het verzoek, maar direct na het verzoek en met alle HTTP-protocolparameters meegezonden naar de webserver.

Het CGI-programma krijgt de informatie via ‘standaard invoer’. Dat wil zeggen dat het voor het CGI-programma lijkt alsof de invoer van het toetsenbord komt (wat uiteraard niet het geval is). Het CGI-programma leest de informatie teken voor teken in en verwerkt deze. Op basis van de gegevens zal het verder op dezelfde manier kunnen handelen als bij een GET-verzoek. Het is ook mogelijk om CGI-programma’s te maken die met beide soorten verzoeken om kunnen gaan. Vaak wordt die mogelijkheid gebruikt om in het geval van een GET-verzoek (de standaard van een internet-browser) een formulier te genereren. De informatie wordt daarna via POST verstuurd.

Belangrijk is dat uw webserver moet weten dat een bepaald bestand een CGI-programma is en als zodanig moet worden uitgevoerd wanneer het wordt aangeroepen. Het kan bepaald worden door de map waarin het programma geïnstalleerd is, maar soms ook door de extensie van de bestandsnaam. Hoe dit exact moet worden aangegeven, hangt af van de configuratie van uw webserver; raadpleeg eventueel de documentatie.

17.7 Een CGI-programma maken

Allereerst mag u kiezen welke programmeertaal u wilt gebruiken. CGI kan worden geschreven in elke willekeurige programmeertaal die op uw platform beschikbaar is. Een zeer veel gebruikte programmeertaal (scripttaal) is Perl. Perl is voor zeer veel besturingssystemen beschikbaar. Daarvan wordt hier een voorbeeld gegeven.

Het eerste dat een CGI-programma moet doen, is aan de webserver vertellen welk soort informatie zal volgen. Hiervoor dient het een regel beginnend met ‘Content-Type:’ te printen. Achter ‘Content-Type:’ volgt het soort informatie:

- webpagina: `text/html`
- platte tekst: `text/plain`
- GIF-afbeelding: `image/gif`
- JPEG-afbeelding: `image/jpeg`
- Word-document: `application/msword`
- enzovoort

Hierna volgen eventueel andere opties, een lege regel en daarna de inhoud.

Een heel eenvoudig CGI-script is het volgende, geschreven in Perl:

```
#!/usr/local/bin/perl
$|=1;
printf “Content-Type: text/html\n”;
printf “\n”;
printf “<html><body><h1>Hello, World!</h1></body></html>\n”;
```

Figuur 217: Script van Perl

Een simpele paginateller, die een klein icoontje teruggeeft als onderdeel van een webpagina, zou er als volgt uit kunnen zien:

```
#!/usr/local/bin/perl
$|=1;
printf “Content-Type: image/gif\n”;
printf “\n”;
system(“cat /home/httpd/icons/count.gif”);
my $COUNT=‘cat /home/httpd/etc/pagecount.txt‘; chop $COUNT;
$COUNT++;
open(STATS, “/home/httpd/etc/pagecount.txt”);
printf STATS “%d\n”, $COUNT;
close STATS;
```

Figuur 218: Perl-script voor paginateller

Dit script leest een bestand met de huidige stand en schrijft de nieuw stand weer weg in dat bestand. Ondertussen stuurt het de inhoud van een GIF-bestandje terug naar de internet-browser.

Een derde voorbeeld laat zien hoe de invoer via een POST-verzoek kan worden verwerkt en zou bij uitvoering een lijstje laten zien van de invoerparameters:

```
#!/usr/local/bin/perl
$|=1;

# Forward declarations
sub http_header;
sub html_start;
sub html_finish;

http_header();
if ($ENV{’REQUEST_METHOD’} ne ‘POST’) {
  html_start(‘Fout’);
  print <<EOM
<h1>Fout</h1>
<p>U  heeft  dit  script  waarschijnlijk  niet  met  het  juist  formulier
aangeroepen</p>
EOM
}
else
{
#-------------------------------------------------------------------------
# Verwerk de invoer
#-------------------------------------------------------------------------
  read(STDIN, $buffer, $ENV{’CONTENT_LENGTH’});
  @pairs = split(/&/, $buffer);
  html_start(‘Invoer’);
  print “<ul>\n”;
  foreach $pair (@pairs) {
     ($name, $value) = split(/=/, $pair);
     # Decodeer de parameters
     $value =~ tr/+/ /;
     $value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack(“C”, hex($1))/eg;
     $value =~ s/<!--(.|\n)*-->//g;

     if ($allow_html != 1) {
        $value =~ s/<([^>]|\n)*>//g;
     }

     printf “<li><b>%s:</b> %s</li>\n”, $name, $value;
  }
  print « </ul>\n »;
};

html_finish();
```

```
exit(0);
```

```
sub http_header {
  print "Content-Type: text/html\n\n";
}

sub html_start {
  my($title) = @_;
  print <<EOM;
<html>
<head>
<title>$title</title>
</head>

<body bgcolor="#FFFFFF">
EOM
}

sub html_finish {
  print <<EOM;
</body>
</html>
EOM
}
```

Figuur 219: Perl-script voor lijst invoer-parameters

De pad- en bestandsnamen in de scripts zullen verschillen bij gebruik op uw eigen machine, zeker wanneer het een Windows- of Macintosh-systeem betreft.

Meer informatie over HTML-formulieren, JavaScript en CGI kunt u vinden op http://developer.netscape.com/.

18. IP-adressering en Network Address Translation

18.1 IP-nummers van netwerk vervangen door IP-nummers van kennisnet

Wanneer u binnen het netwerk van uw eigen organisatie al IP-nummers hebt toegekend, moet u deze toch vervangen door de IP-nummers van kennisnet. De reeks IP-nummers die men krijgt, is immers afhankelijk van de IP-leverancier. Ook kennisnet is zo´n IP-leverancier en heeft een eigen nummerreeks.

Dit hoeft geen groot probleem op te leveren. Alle werkstations kunnen in principe met DHCP worden geconfigureerd (zie deel III voor instructies), zodat de IP-nummers daarvoor automatisch via kennisnet worden verkregen. Alleen eigen servers, LAN-servers bijvoorbeeld, of interne routers *moeten* worden voorzien van vaste (statische) IP-nummers.

18.2 De eigen IP-adressen toch behouden

In principe kunt u de eigen IP-adressen niet behouden. U krijgt van kennisnet een reeks adressen toegewezen, die u dient te gebruiken. Er bestaat echter een truc, NAT (Network Address Translation) of ‘masquerading’ genoemd, waarmee het mogelijk is om uw interne IP-nummers naar de IP-nummers van kennisnet te vertalen, en weer terug. Er zit ook een schaduwzijde aan NAT of masquerading: niet alle diensten kunnen op deze manier worden gebruikt, doch de belangrijkste diensten wel.

Indien u van NAT of masquerading gebruik wilt maken, is dit geheel uw eigen verantwoordelijkheid en dient u zelf voor de extra apparatuur en programmatuur én het onderhoud daarvan te zorgen. U plaatst dan een eigen ‘router’ of ‘forwarding host’ (computer) tussen de kennisnetaansluiting en uw lokale netwerk.

Een andere oplossing zou kunnen zijn om alle applicaties die u wilt gebruiken, via een proxy te laten lopen. Hiertoe dient u zelf een proxy-server op te zetten die geen routering van IP ondersteunt, of waarop routering (soms ook ‘forwarding’ genoemd) in ieder geval is uitgeschakeld. Voor websurfen maakt u gebruik van een HTTP-proxy. Voor veel andere protocollen zoals Telnet, Secure Shell (SSH), het ophalen en verzenden van e-mail en IRC kan, indien uw software dit ondersteunt, gebruik worden gemaakt van SOCKS. Er zijn diverse proxy-pakketten op de markt verkrijgbaar. Via Tucows kunt u, in elk geval voor Windows NT, een aantal commerciële demoversies van dergelijke pakketten ophalen.

Let er wel op dat uw netwerken in dit geval ‘logisch’ gescheiden zijn en veel speciale protocollen niet worden ondersteund door proxy-servers.

18.3 De werking van ‘Network Address Translation’ (NAT)

Network Address Translation, kortweg NAT, zorgt ervoor dat adressen aan de ene kant van een router worden vertaald naar adressen aan de andere kant van de router, zodat er verkeer mogelijk wordt gemaakt door de router. Dit kan nuttig zijn wanneer u op een lokaal netwerk adressen gebruikt die normaliter niet bruikbaar zijn buiten het lokale netwerk.

Er zijn verschillende vormen van NAT: 1-op-1-vertaling, 1-op-*n*-vertaling en *n*-op-*m*-vertaling. Meer informatie kunt u vinden in een afstudeerscriptie van een Duitse student:

http://www.csn.tu-chemnitz.de/~mha/linux-ip-nat/diplom/.

In dit Engelstalige document wordt duidelijk en zeer gedetailleerd uitgelegd hoe de verschillende vormen van NAT werken.

De meest voorkomende variant van NAT is ‘masquerading’, waarbij alle adressen van het interne netwerk worden vertaald naar slechts één IP-adres aan de buitenkant van het netwerk.

18.4 De beperkingen van NAT/masquerading

Het gebruik van NAT wordt over het algemeen door de experts niet aangeraden. NAT is een truc en geen oplossing voor de lange termijn. NAT is onder meer bedoeld om problemen met de schaarste van IP-adressen op te vangen en om het eenvoudiger te maken om een aansluiting te verhuizen (zonder het interne netwerk te hoeven omnummeren). De reden dat NAT of masquerading ondanks deze voordelen wordt afgeraden, heeft ermee te maken dat niet alle protocollen bestand zijn tegen adresvertaling. Soms is dit op te lossen, maar niet altijd.

Een bekend voorbeeld is FTP. Overigens is het probleem in dit geval in nagenoeg alle NAT-implementaties opgelost. Ter illustratie wordt hier uitgelegd wat er gebeurt tijdens het FTP'en.

FTP maakt gebruik van twee verbindingen. Allereerst wordt een verbinding opgezet om de overdracht van bestanden en informatie te bedienen ('Control Channel'). Telkens wanneer er een bestand of informatie opgevraagd of verzonden moet worden, wordt er een tweede verbinding opgezet ('Data Channel'). Het IP-adres en het TCP-poortnummer van het 'Control Channel' worden bepaald door de server en zijn een vast gegeven, maar het IP-adres en het TCP-poortnummer van het 'Data Channel' worden dynamisch bepaald door de clientapplicatie.

Om het 'Data Channel' te openen, stuurt de applicatie het volgende commando (de getoonde getallen zijn slechts voorbeelden):

```
PORT 10,1,1,153,8,24
```

Dit commando heeft zes parameters, gescheiden door komma's. De eerste vier parameters vormen samen de vier delen van het IP-adres: **10**.**1**.**1**.**153**. De laatste twee parameters vormen samen het betreffende TCP-poortnummer: **8***256 + **24** = 2072.

De FTP-server zal op dat moment dus een verbinding proberen te maken met het IP-adres 10.1.1.153 op TCP-poort 2072. Indien dat slaagt, volgt het volgende antwoord:

```
200 PORT command successful.
```

Indien er een NAT-systeem tussen zou zitten, zou de applicatie een intern en onbereikbaar adres doorgeven in het PORT-commando. Het adres van de NAT-gateway (aan de buitenkant) is bijvoorbeeld 212.178.1.1 en dat is het enige adres dat de FTP-server kan bereiken. Wanneer de FTP-server een verbinding zou proberen op te zetten met 10.1.1.153, zou dat niet lukken.

Om te voorkomen dat de FTP-server met 10.1.1.153 zou verbinden, moet de NAT-gateway actief het FTP-verkeer op het 'Control Channel' in de gaten houden. Wanneer er een PORT-commando voorbijkomt, dient dit te worden afgevangen. De NAT-gateway vervangt de eerste vier parameters, zodat het IP-adres 212.178.1.1 wordt vermeld. De NAT-gateway bepaalt zelf een willekeurig poortnummer en vult dat in voor de laatste twee parameters. Het resultaat wordt dan bijvoorbeeld:

```
PORT 212,178,1,1,235,74
```

Wanneer de FTP-server dan een 'Data Channel' opzet naar 212.178.1.1, TCP-poort (235*256+74=) 60234, maakt de NAT-gateway een verbinding met 10.1.1.153, TCP-poort 2072 en stuurt het verkeer tussen de beide verbindingen door.

Om te zorgen dat de NAT-gateway deze truc kan uitvoeren, zijn extra controles nodig op het verkeer. Dit maakt de NAT-gateway een stuk complexer. Een dergelijke truc kan helaas niet voor alle protocollen worden uitgehaald, zeker niet wanneer het verkeer wordt gecodeerd. Soms biedt een (SOCKS-)proxy -server in dat geval uitkomst.

18.5 Meer IP-nummers krijgen voor kennisnet

Als u meent dat u te weinig IP-nummers hebt gekregen, kunt u er in bepaalde gevallen meer krijgen. Dat kan indien u de noodzaak ervan kunt aantonen. Hiertoe dient u een *beargumenteerd* en *gespecificeerd* verzoek in te dienen bij het Servicepunt Kennisnet op het internet-adres: http://servicepunt.kennisnet.nl/.

RIPE-NCC, de autoriteit die voor Europa verantwoordelijk is voor de uitgifte van (publieke) IP-adressen, heeft vrij strikte regels opgesteld voor het gebruik van IP-adressen. Deze regels vereisen dat wordt beargumenteerd dat extra IP-adressen daadwerkelijk noodzakelijk zijn.

Houdt u er rekening mee dat u bepaalde instellingen in uw netwerk zult moeten aanpassen, omdat niet kan worden gegarandeerd dat de nieuwe nummers aansluiten op de thans aan u toegewezen reeks.

19. Netwerkkoppelingen

19.1 De eigen internet-webserver koppelen via kennisnet

U kunt de eigen internet-webserver via kennisnet koppelen. Via een 'reverse proxy' (zie hoofdstuk 15) kan vanaf kennisnet toegang worden verkregen tot de webserver van uw organisatie. U dient een verzoek in te dienen bij het Servicepunt Kennisnet om dit voor u te realiseren op het internet-adres: http://servicepunt.kennisnet.nl/.

U dient hiervoor, eveneens via het Servicepunt Kennisnet, een eigen domeinnaam aan te vragen indien u hierover nog niet beschikt.

19.2 Via de modempool van de organisatie het kennisnet op

Het is in principe *niet* de bedoeling dat gebruikers kennisnet opgaan via de modempool van de organisatie. Het netwerk van kennisnet is opgezet als een gesloten netwerk en dat zal ook zo blijven. Door een modempool aan het schoolnetwerk te koppelen, creëert u een 'achterdeur' naar het kennisnet. Alleen indien u kunt *garanderen* dat er doormiddel van een aanmelding met minimaal een gebruikersnaam en wachtwoord tot uw netwerk toegang kan worden verkregen *én* kunt *garanderen* dat er geen andere gebruikers dan de bestaande gebruikers van kennisnet via uw inbelvoorziening het kennisnet op kunnen, is het toegestaan om een dergelijke voorziening aan uw leerlingen aan te bieden.

19.3 De eigen internet-aansluiting in combinatie met kennisnet

Als uw organisatie al een eigen internet-aansluiting heeft, moet u ten behoeve van de aansluiting op kennisnet een en ander regelen. Als u al druk gebruikmaakt van uw bestaande aansluiting, is het raadzaam de nieuwe kennisnetaansluiting eerst met een aantal werkstations uit te proberen en dan rustig een migratie te plannen naar een situatie met alleen nog een kennisnetaansluiting. Overleg met het Servicepunt Kennisnet is daarbij onontbeerlijk.

In de situatie dat u beide aansluitingen naast elkaar gebruikt, dient u ervoor te zorgen dat er geen vermenging optreedt. Dat betekent dat een lokaal systeem *of* met kennisnet moet praten, *of* met de andere aansluiting – verwarring moet niet mogelijk zijn. *Er mag op geen enkele manier contact ontstaan tussen uw internet-aansluiting en uw aansluiting op kennisnet!*

Let op!

Er mag slechts één DHCP-service tegelijk actief zijn, dus als uw bestaande aansluiting ook DHCP biedt (automatische IP-nummertoekenning), dan móet dat in de kennisnetaansluiting worden uitgezet (zie hoofdstuk 13).

Als u meteen wilt overstappen, is het raadzaam om de bestaande aansluiting uit te schakelen, zodat eventuele conflicten worden vermeden.

Bij het gebruik van twee aansluitingen tegelijk bent u geheel verantwoordelijk voor mogelijke beveiligingsrisico's die u voor kennisnet introduceert ('achterdeurtjes').

Nogmaals: in situaties als deze is overleg met het Servicepunt Kennisnet onontbeerlijk!

19.4 Gevolgen van eigen routers in het lokale netwerk

Als er in het lokale netwerk eigen routers zijn die verschillende delen met elkaar verbinden, dan heeft dit gevolgen. De computers die zich ‘achter’ deze router(s) bevinden, dienen de betreffende router als ‘default gateway’ te gebruiken, in plaats van de gateway die via de centrale DHCP-server van kennisnet wordt doorgegeven. Dit kunt u ‘hard’ instellen in uw clients, maar beter is waarschijnlijk (afhankelijk van het aantal clients) om een eigen DHCP-server op te zetten, die de juiste gegevens uitdeelt. Zie hiervoor hoofdstuk 13.

Eigenlijk is het gebruik van routers in uw eigen netwerk niet nodig, althans in het geval van een lokaal netwerk, dat behalve de kennisnetaansluiting geen verbindingen heeft met bijvoorbeeld andere locaties van de school. Elke vestiging hoort een eigen kennisnetaansluiting te hebben. Veel beter is het om op de locaties zelf een aantal grotere hubs of switches te gebruiken om verschillende segmenten te koppelen. Deze zijn over het algemeen een stuk goedkoper dan routers en vergen beduidend minder, of zelfs geen onderhoud.

U mag in geen geval (met behulp van routers) verbindingen maken met IP-netwerken die níet tot kennisnet behoren.

20. Literatuur

- Telemark Systems, Inc.; “NT DNS Configuration - using BIND 4.9.3 Release”; Telemark Systems, Inc., april 1996; http://www.telemark.net/~randallg/ntdns.htm .
- Langfeldt, Nicolai <janl@math.uio.no>; “DNS-HOWTO” (Linux HowTo); Langfeldt, Nicolai, 1995-1999; http://metalab.unc.edu/pub/linux/docs/howto/DNS-HOWTO.

Handboek

Aansluiting van het schoolnetwerk op kennisnet

Deel VI: Beveiliging en veiligheidsmaatregelen

Indeling van deel VI

Hoofdstuk 21 gaat over

- beveiliging in het algemeen,
- wat u kunt doen bij een beveiligingsprobleem
- wat u kunt doen om beveiligingsproblemen te voorkomen.

Hoofdstuk 22 gaat over

- de beveiliging op kennisnet,
- de beveiliging van uw schoolaansluiting
- risico's voor de veiligheid van uw netwerk.

21. Beveiliging en veiligheidsprocedures

Het is uiterst belangrijk dat de veiligheid van kennisnet en van uw computers en werkstations is gewaarborgd. Dit gebeurt op basis van richtlijnen en algemeen gebruikte werkwijzen ('common practice') die door het Ministerie van Onderwijs, Wetenschappen en Cultuur zijn vastgesteld.

Het landelijke netwerk wordt beschermd door middel van een firewall die alleen verkeer door laat dat expliciet is toegestaan. Routers van schoolnetwerken zijn voorzien van extra beveiligingsregels die bepaald netwerkverkeer blokkeren.

Aangezien kennisnet erg omvangrijk wordt en aangezien er regelmatig beveiligingsfouten in systeemsoftware worden ontdekt, kunnen zich toch incidenten voordoen. Daarom is voor kennisnet een team samengesteld dat kan adviseren en assisteren bij het analyseren van veiligheidsincidenten. Waar nodig zal dit team maatregelen nemen, voorzover dit technisch, organisatorisch en wettelijk mogelijk is.

Het aanspreekpunt voor veiligheidsincidenten is het Servicepunt Kennisnet (zie bijlage A, in deel VII). Zij hebben voor u de benodigde formulieren en kunnen u informeren hoe u een juiste rapportage maakt van het incident en welke instanties u verder nog kunt inschakelen.

[Informatie en inspiratie voor dit hoofdstuk is onder andere afkomstig uit de 'Computer Forensics Class 1999' van Wietse Veenema en Dan Farmer: http://www.fish.com/forensics.]

21.1 Veiligheidsincident: procedures

Als u vermoedt dat een systeem op uw netwerk is of wordt aangevallen, moet u de volgende acties ondernemen:

- Stel zoveel mogelijk informatie veilig. Alle logbestanden die u kunt vinden moet u opslaan op een extern opslagmedium of een ander computersysteem. Op Unix-systemen kunt u de logbestanden meestal vinden in de map `/var/log` of `/var/logs`.
- Probeer de bron van de aanval te achterhalen. Controleer hiertoe actieve netwerkverbindingen en -sessies. Dit kunt u doen met het commando 'netstat'. Dit commando geeft informatie over openstaande IP-sessies. Als u aan dit commando de optie '-a' toevoegt, ziet u *alle* open verbindingen. Als u aan dit commando de optie '-n' toevoegt, ziet u alleen een numerieke weergave. De optie '-n' voorkomt dat er een DNS-controle wordt gedaan, die het beeld kan verstoren. Hieronder volgt een voorbeeld.

Windows	*Unix/Linux*
Voorbeeld:	Voorbeeld:
`C:\> netstat -a -n`	`$ netstat -an`
Als u de optie '/?' toevoegt, krijgt u meer informatie over dit commando.	Als u het commando 'netstat --help' of 'man netstat' invoert, krijgt u meer informatie over dit commando.

Figuur 220: Commando 'netstat'

- Ontkoppel zonodig het desbetreffende systeem van het netwerk door de netwerkkabel te ontkoppelen. Dit kan echter wel de opsporing van de dader bemoeilijken of onmogelijk maken, zeker als het een geval van 'heterdaad' is.

- 'Bevries' het systeem, zodat het geheugen, de schijf en geheugenbuffers (caches) en de status van de harde schijf onveranderd blijven. Voor nadere analyse is het belangrijk om het systeem zoveel mogelijk te laten als het is. Elke handeling die u uitvoert, kan namelijk invloed hebben op de status van het systeem en onderdelen ervan. U kunt gebruikmaken van het programma 'Advanced Power Management'. Sommige systemen kunnen het geheugen naar een speciale partitie op de harde schijf wegschrijven en zo de status van het systeem vastleggen. Dit betreft echter voornamelijk laptop-computers en slechts sporadisch servers.
- Maak een volledige back-up van uw systeem, vooral als Advanced Power Management geen uitkomst kan bieden.
- Neem contact op met het Servicepunt Kennisnet (zie bijlage A, in deel VII) om het incident te melden. Het Servicepunt Kennisnet kan vervolgens contact opnemen met de juiste instanties.
- Neem tevens contact op met uw netwerkleverancier en/of -beheerpartij om na te gaan welke mogelijkheden zij hebben om het incident te analyseren en schade te herstellen.

Let op 1!

Als uw systeem is getroffen door een 'Trojaans paard'[18], kan dat betekenen dat uw systeem van de grond af moet worden opgebouwd met behulp van de installatiediskettes of cd-rom's. Trojaanse paarden kunnen geruime tijd op uw systeem actief zijn voordat ze toeslaan. Als u geluk hebt, kunt u de grootste schade herstellen door back-ups van enkele maanden oud terug te zetten.

Let op 2!

Het is heel belangrijk om juiste en complete informatie te hebben. Deze informatie kan komen uit logbestanden, systeeminformatiesoftware, hulpmiddelen, handleidingen, enzovoort. Logbestanden en informatie van systeeminformatiesoftware (netwerkstatus, actieve processen) moet zijn voorzien van datum en tijd. Deze tijd moet correct zijn en voorzien van de juiste tijdzoneaanduiding. Maak voor uw belangrijke servers daarom gebruik van een tijdserver (zie deel III).

21.2 Inbraak op uw systeem: procedures

Als u vermoedt dat op een systeem op uw netwerk is of wordt ingebroken, moet u de volgende acties ondernemen.

- Ga na of het wellicht geen inbraak is, maar een softwarefout of een computervirus.

Als u ervan bent overtuigd dat het een inbraak betreft, moet u het volgende doen:

- Verzamel zoveel mogelijk informatie. Doe dit zo mogelijk zonder dat de 'inbreker' hiervan iets merkt.
- Stel zoveel mogelijk informatie veilig. A*lle* logbestanden die u kunt vinden moet u opslaan op een extern opslagmedium of een ander computersysteem. Op Unix-systemen kunt u de logbestanden meestal vinden in de map `/var/log` of `/var/logs`.
- Ontkoppel indien nodig het desbetreffende systeem van het netwerk door de netwerkkabel te ontkoppelen. Dit kan echter wel de opsporing van de dader bemoeilijken of onmogelijk maken, zeker als het een geval van 'heterdaad' is.

[18] 'Trojan Horse', naar analogie van de legende van het paard van Troje: een type computervirus, dat zich via een op zichzelf onschuldig lijkend programma in uw systeem nestelt en vrij onverwacht toeslaat.

- Neem contact op met het Servicepunt Kennisnet (zie bijlage A, in deel VII) en probeer daarbij zoveel mogelijk relevante informatie te verstrekken. Wacht niet te lang met melden: misschien is het mogelijk de dader op heterdaad te betrappen. Het beveiligingsteam van kennisnet kan u hierbij helpen. U kunt hen bereiken via het Servicepunt Kennisnet (0800-KENNISNET/ 0800-536647638), keuze/optie 3, of per e-mail via 'security@kennisnet.nl'.



21.3 Portscan

Een 'portscan' vindt plaats als iemand kortstondig een verbinding maakt met een poort en deze verbinding direct weer verbreekt. Er wordt dus niet ingebroken of aangemeld onder valse voorwendselen. Op zich hoeft een portscan geen gevaar te zijn voor de veiligheid van uw systemen. Het kan echter wel zijn dat iemand probeert om bijvoorbeeld gevoelige systemen en netwerkdiensten te vinden.

Als u een portscan ontdekt, moet u het volgende doen:

- Zoek uit welke poorten zijn gescand.
- Ga na of de gescande poorten mogelijk 'bijzondere' poorten zijn, die door 'hacker-tools' kunnen worden gebruikt of die bij applicaties horen waarvan recent beveiligingsproblemen zijn gemeld. Als dit het geval blijkt, neem dan contact op met het Servicepunt Kennisnet (zie bijlage A, in deel VII).

21.4 Voorkomen van veiligheidsincidenten en schade

Veel incidenten worden veroorzaakt doordat 'crackers' gebruikmaken van fouten in netwerk- en systeemsoftware. In verband hiermee kunnen de volgende tips worden gegeven.

U kunt de kans op veiligheidsincidenten verkleinen door de volgende acties te ondernemen:

- Gebruik de meest recente stabiele versie van netwerk- en systeemsoftware en gebruik de nieuwste 'patches' (lapmiddelen). Deze patches zijn meestal te downloaden van de websites van de softwareproducenten.
- Gebruik alleen software van betrouwbare bronnen, dus rechtstreeks van uw leverancier of van vertrouwde websites.
- Installeer een virusscanner en neem bij voorkeur een abonnement om regelmatig verse antivirusinformatie te ontvangen van de producent.
- Zorg ervoor dat zo min mogelijk software op uw systemen is geïnstalleerd en geactiveerd. Installeer alleen de software die nodig is voor het normaal functioneren van het systeem. Activeer alleen die programmatuur, die noodzakelijk is om de diensten die u wilt leveren, te kunnen uitvoeren.
    - Als u werkt met Windows NT, raden wij u aan om alle niet-noodzakelijke 'Network Services' uit te schakelen.
    - Als u werkt met Linux (RedHat of SuSe) kunt u met de 'Runlevel Editor' aangeven welke processen en diensten het systeem moet starten.

- Controleer regelmatig of er verdachte processen op uw computer actief zijn. Dit kunt u doen door een proceslijst op te vragen[19].
- Controleer regelmatig of er verdachte netwerkpoorten in gebruik zijn. Dit kunt u doen met het commando 'netstat' (Windows of Unix/Linux) (zie paragraaf 21.1). Hiervoor is wel enige kennis van netwerksoftware en poortnummers nodig. Een nuttige bron van informatie kan de lijst van 'assigned numbers' zijn:

  http://www.isi.edu/in-notes/iana/assignments/port-numbers.
- Controleer regelmatig uw logbestanden op verdachte zaken. Voor bepaalde typen logbestanden en besturingssystemen is analysesoftware beschikbaar op onder meer de websites http://www.tucows.com, http://www.software.com en http://www.download.com.
- Maak regelmatig, liefst dagelijks, back-ups van uw vitale computersystemen – *ook van uw log- en configuratiebestanden.*
- Laat het onderhoud en beheer van uw systemen eventueel uitvoeren door een derde die is gespecialiseerd in de beveiliging van computersystemen.
- Blijf op de hoogte van probleemrapportages van de software die u gebruikt. Dit kunt u doen door zich te abonneren op een zogenaamde mailinglist of nieuwsbrief van bijvoorbeeld een gebruikersgroep of van de producent van de software. Een andere mogelijkheid is om regelmatig websites en/of nieuwsgroepen over dit onderwerp te raadplegen.
  - http://www.cert.org/advisories/
  - http://www.rootshell.com
  - http://www.insecure.org
  - http://www.ntsecurity.net/

21.5 Hackers en crackers

Een 'hacker' is iemand die handig is in het schrijven van software en goed met computers overweg kan. Een 'hacker' heeft de mogelijkheid en kennis om systemen te kraken, maar niet de intentie. De term 'hacken' wordt ook wel gebruikt voor (even gauw) iets programmeren.

Een 'cracker' daarentegen is minder onschuldig. Een 'cracker' is ook erg handig, maar gebruikt deze handigheid om systemen te kraken (in te breken), mogelijk gegevens te stelen, te vernietigen of te corrumperen.

In de volksmond wordt aan de term 'hacker' meestal de betekenis van 'cracker' toegekend.

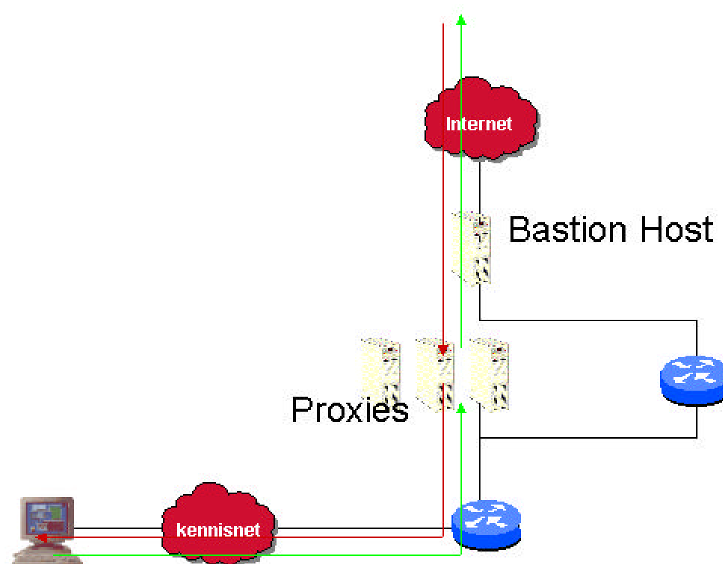
[19] Onder Windows 95/98 en NT is de lijst met actieve programma's *niet* voldoende om inzicht te krijgen in de werkelijk actieve software. Hiervoor moet u in ieder geval het programma 'Systeeminfo' uitvoeren.

22. Beveiliging kennisnet

22.1 Beveiliging met proxy-servers

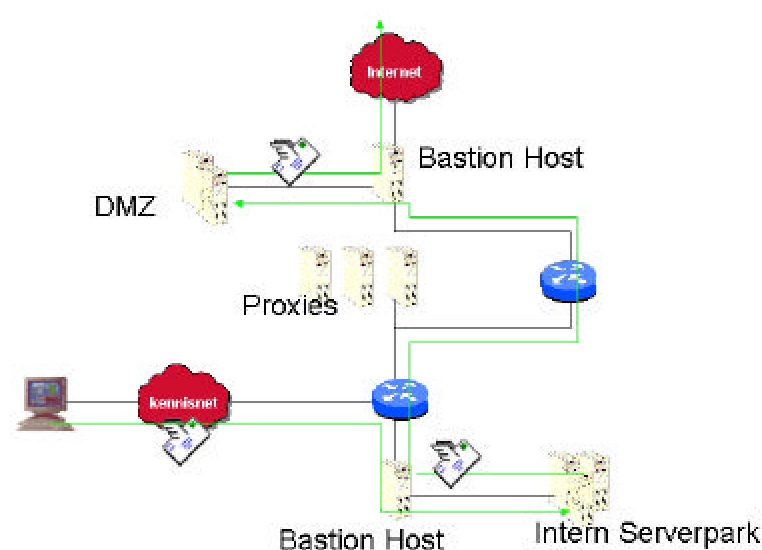
Kennisnet is beveiligd met behulp van proxy-servers en relay-servers. Al het verkeer tussen kennisnet en het internet loopt via deze servers. Er is dus geen rechtstreeks verkeer van binnen naar buiten, of andersom.

De proxy-servers zijn bedoeld om vanuit kennisnet toepassingen mogelijk te maken waarvoor u normaal een rechtstreekse verbinding met de eindbestemming zou opzetten. Het gaat om toepassingen als het web, FTP, RealAudio/Video (film, muziek en radio via het internet), Telnet en IRC.



Figuur 221: Proxy-structuur

De relay-servers zijn bedoeld voor diensten waarvoor niet altijd een rechtstreekse verbinding met de eindbestemming moet worden opgebouwd, zoals e-mail en nieuwsgroepen.



Figuur 222: Mailrelays

Door deze beveiligingsmaatregelen is het in principe niet mogelijk dat iemand vanaf het internet rechtstreeks uw systemen of de interne systemen van kennisnet benadert.

22.2 Beveiliging (school)aansluiting

De aansluiting van uwschool of andere organisatie is beveiligd met behulp van de router. U bent aangesloten op kennisnet met een router, een kabelmodem of een gecombineerd systeem. In ieder geval bevat uw aansluiting routingfunctionaliteit. De router kan selecteren welk verkeer wel en welk verkeer niet van en naar uw lokale netwerk mag.

Alle schoolrouters zijn voorzien van filters. Deze filters delen de IP-reeks van uw schoolnetwerk in stukken (zie ook Bijlage B, in deel VII). De IP-reeks bestaat uit de router, een gereserveerd adres en de volgende drie groepen:

- werkplekken;
- servers die op kennisnet ‘zichtbaar’ moeten zijn;
- servers en apparatuur die *uitsluitend* bereikbaar mogen zijn vanaf uw lokale netwerk.

Voor elk van deze groepen geldt een andere manier van filteren. Het filteren geschiedt op basis van het IP-adres (het unieke adres op het internet) van de systemen en de zogenoemde poortnummers. Poorten worden gebruikt door applicaties om de verbindingen te identificeren. Een verbinding tussen twee systemen is uniek geïdentificeerd door het IP-adres en poortnummer van elke kant van de verbinding.

22.2.1 Werkplekken

Uitgaande sessies (dus geïnitieerd vanaf een werkstation op uw lokale netwerk) vinden normaliter alleen plaats vanaf een poort hoger dan 1023 (dit zijn de ‘hoge poorten’), de meest belangrijke applicaties gebruiken ‘lage poorten’ (1-1023). Voor werkstations, die over het algemeen geen applicaties behoren aan te bieden, is het netwerk op de lage poorten afgeschermd. Hierdoor kan vrijwel alleen verkeer binnenkomen dat is geïnitieerd vanuit uw eigen netwerk.

22.2.2 Servers die op kennisnet ‘zichtbaar’ moeten zijn

Deze servers staan in principe open voor inkomend verkeer, zodat u diensten aan kennisnet en kennisnetgebruikers kunt aanbieden, of systemen bereikbaar kunt maken vanaf kennisnet. Zo kunt u in deze reeks uw eigen webserver of mailserver plaatsen.

22.2.3 Servers en apparatuur die uitsluitend en alleen bereikbaar mogen zijn vanaf uw lokale netwerk

Deze groep is volledig afgeschermd. Er komt geen bit informatie doorheen.

22.2.4 Maatregelen voor gehele IP-adresreeks

Naast deze maatregelen voor specifieke groepen gelden voor de gehele IP-adresreeks de volgende maatregelen.

- *NetBIOS gesloten*

  NetBIOS is het protocol waarmee Windows-systemen onderling bestanden uitwisselen en afdrukopdrachten naar printers sturen. Dit protocol en de implementatie ervan blijken niet waterdicht te zijn en gevoelig voor inbraak. Daarom wordt NetBIOS gesloten voor het kennisnet.

- *Standaard cracking-poorten gesloten*

  Veel ‘cracking-tools’, zoals BackOrifice en NetBus, komen meestal als een ‘Trojaans Paard’ binnen. Deze cracking-tools maken vaak gebruik van standaardpoorten. Deze poorten zijn dichtgemaakt. U bent hiermee echter *niet* beveiligd tegen aanvallen van buitenaf via andere poorten.

- *Beveiliging tegen ‘broadcast’*

  Kennisnet is beveiligd tegen ‘broadcasts’. Een ‘broadcast’ is een signaal naar een speciaal IP-adres in uw IP-reeks, het broadcastadres. Op zo’n signaal kunnen theoretisch *alle* computersystemen op uw netwerk reageren. Een voorbeeld is de Smurf-aanval, waarbij uw netwerk als een versterker fungeert. De Smurf-aanval stuurt een reeks pakketjes naar uw netwerk met een vervalst afzenderadres. De systemen op uw netwerk reageren hierop en sturen dan massaal een antwoord naar het valse afzenderadres, waardoor uw netwerkverbinding en de ontvanger van de antwoorden het erg druk krijgen.

22.3 Risico’s voor de veiligheid

Het is niet mogelijk om 100% veiligheid voor uw netwerk te garanderen. Er zijn namelijk diverse gevaren, waartegen kennisnet moeilijk iets kan doen.

- *Virussen*

  De bestrijding van virussen loopt eigenlijk altijd achter de feiten aan. Voordat een ‘vaccin’ kan worden gemaakt door de producenten van antivirussoftware, moet het virus eerst een tijd actief zijn. Virussen die zich verspreiden via e-mail (zoals ‘Melissa’ en ‘I Love You’) werken vaak erg snel. Let daarom op het volgende:

  - Open verdachte aanhangsels van e-mail niet.
  - Download alleen software van vertrouwde web- en FTP-sites.
  - Geef bovenstaande instructies ook aan uw gebruikers door.

- *Fouten in software*

  Software is zelden foutvrij. Grote programma’s zonder fouten bestaan al helemaal niet. Regelmatig worden fouten ontdekt in software, die kleine of grote gevolgen kunnen hebben voor de beveiliging van computersystemen. Het gaat vaak om situaties die zelden voorkomen, maar *als* ze voorkomen, kan soms gehele of gedeeltelijke controle over het desbetreffende systeem worden verkregen. Als er bijvoorbeeld een ‘lek’ in uw webserver zit en iemand maakt daar vanaf kennisnet of vanaf het internet gebruik van, kan dat de veiligheid van uw webservice tenietdoen. Houd daarom uw software actueel en breng alle door de leverancier geadviseerde beveiligingen aan. Activeer *nooit* meer diensten dan absoluut noodzakelijk.

- *Kwaadwillende eigen gebruikers*

  Ook uw eigen gebruikers kunnen een gevaar vormen voor de veiligheid van uw systemen. Veel aanvallen op computersystemen vinden plaats van binnenuit. Om risico’s te verkleinen kunt u het volgende doen:

  - Scheid uw administratieve netwerk (fysiek of via een eigen firewall) van het leerlingennetwerk en de kennisnetkoppeling.
  - Maak op een separaat systeem een kopie van gegevens die zowel op het administratienetwerk als het leerlingennetwerk beschikbaar moeten zijn.
- *'Verloren' wachtwoorden*

  Een veelvoorkomend probleem is dat wachtwoorden worden gekraakt of achterhaald. Dit kan gebeuren als uw wachtwoord te eenvoudig is of bij teveel mensen bekend is. Als u een wachtwoord met veel mensen deelt, kan het een eigen leven gaan leiden. Doe daarom het volgende:

  - Neem een wachtwoord dat niet voor de hand ligt maar dat u wel eenvoudig kunt onthouden.
  - Schrijf uw wachtwoord *niet* op.
- *Cracking-tools*

  Een cracking-tool is eigenlijk een soort virus, omdat veel cracking-tools als 'Trojaanse Paarden' binnenkomen. In de beveiligingsfilters in de routers zijn maatregelen genomen tegen cracking-tools als BackOrifice en Netbus, maar deze beveiliging geldt alleen voor de standaardpoorten. Het is onmogelijk om alle poorten van het netwerk te sluiten, want dat zou betekenen dat uw complete netwerk wordt gesloten. Ook komen er steeds nieuwe 'tools' bij die weer andere poortnummers gebruiken. Het duurt dus enige tijd voordat alles weer kan worden bijgesteld. Ook hier geldt: voorkomen is beter dan genezen; probeer waar mogelijk te voorkomen dat uw systemen dergelijke 'virussen' oplopen.

Handboek

Aansluiting van het schoolnetwerk op kennisnet

Deel VII: Veelvoorkomende vragen

Indeling van deel VII

Dit deel behandelt een aantal veelgestelde vragen over kennisnet en de diensten die kennisnet aanbiedt.

Hoofdstuk 23 behandelt vragen over e-mail.

Hoofdstuk 24 behandelt vragen over surfen op internet (het wereldwijde web).

Hoofdstuk 25 behandelt vragen over etiquette op het internet en kennisnet.

Hoofdstuk 26 behandelt een aantal veelvoorkomende problemen.

Hoofdstuk 27 behandelt vragen over aanvullende diensten en over uitbreiding of aanpassing van de dienstverlening van kennisnet.

Hoofdstuk 28 is een bijlage over belangrijke adressen en telefoonnummers voor kennisnet.

Hoofdstuk 29 is een bijlage over het programma Squid voor het koppelen van proxy-servers.

Hoofdstuk 30 is een bijlage over FrontPage.

Hoofdstuk 31 is een bijlage over de indeling van IP-adresreeksen.

23. E-mail

23.1 Hoe kom ik aan de mailadressen voor mijn school of organisatie?

U ontvangt per post een brief met daarin de gegevens (gebruikersnaam, wachtwoord, mailadres) van de ICT-coördinator. In deel IV leest u wat de ICT-coördinator daarna moet doen om de Kennisnet Gebruikersadministratie te onderhouden.

23.2 Hoe koppel ik mailadressen en gebruikersnamen aan personen?

Deel IV behandelt de Kennisnet Gebruikersadministratie voor het beheren van gebruikers binnen uw organisatie. Hieronder valt het koppelen van gebruikersnamen en mailadressen aan personen. U vindt daar ook hoe u wachtwoorden kunt wijzigen.

23.3 Ik kan geen e-mail ophalen. Wat moet ik doen?

Als u geen e-mail kunt ophalen, moet u de volgende stappen ondernemen:

- Controleer alle instellingen van uw e-mailprogramma, zoals gegeven in deel III. Pas zonodig de instellingen aan.
- Als het dan nog niet lukt, controleert u of u een verbinding hebt met de mailservers. U kunt dit doen door met een speciaal programma[20] een 'ping' uit te voeren naar '`pop.kennisnet.nl`' of '`imap.kennisnet.nl`'.
- Controleer vervolgens of u de juiste gebruikersnaam en het juiste wachtwoord hebt ingevoerd.
- Als u uw mail nog steeds niet kunt ophalen, noteert u de foutmelding nauwkeurig en belt u het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28).

23.4 Wat is POP(3) en wat is IMAP(4)? Wat is het verschil?

POP3 en IMAP4 zijn beide protocollen voor het ophalen en lezen van e-mail.

POP3 is de derde en meest actuele versie van het 'Post Office Protocol'.

IMAP4 is de vierde en meest actuele versie van het 'Internet Mail Access Protocol'. Het verschil zit in het doel waarvoor het protocol wordt gebruikt. POP3 is vooral bedoeld om post op te halen naar de lokale computer, daar op te slaan en vervolgens van de server te verwijderen. Alle verdere bewerkingen vinden plaats op de lokale machine. Om post op te slaan in mappen, moet u in het lokale e-mailprogramma mappen maken.

IMAP4 is vooral bedoeld om de berichten op de server achter te laten. IMAP4 kan de berichten op de server in verschillende mappen indelen. IMAP4 kent zowel mappen op de server als lokale mappen (op de eigen computer), waartussen u de berichten kunt verplaatsen. Zo kunt u zelf bepalen waar u uw berichten wilt opslaan, afhankelijk van bijvoorbeeld de beschikbare schijfruimte.

POP3 kan ook berichten (tijdelijk) op de server achterlaten ('leave on server'), maar u kunt niet zoals bij IMAP4 de berichten tussen lokale mappen en mappen op de server verplaatsen.

23.5 Wat is 'SPAM' en wat doe ik ermee?

SPAM is ongewenste en/of ongevraagde e-mail, in het Engels 'unsollicited mail'. Dit zijn vaak berichten die uitnodigen om websites te bezoeken, meestal sites voor volwassenen. Verder gaat het om reclame, aanbiedingen om geld te verdienen met kettingbrieven, enzovoort. Verwijder deze berichten direct. Informeer eventueel de beheerder van het domein waarvandaan de berichten komen, zodat deze maatregelen kan nemen. Het vereist echter gedegen kennis van e-mail om de werkelijke zender te achterhalen.

[20] Er zijn diverse gratis hulpmiddelen te krijgen, bijvoorbeeld 'NetLab' voor Windows, dat u via http://tucows.a2000.nl/ of http://www.tucows.com/ kunt vinden, of OTTool voor de Macintosh.

‘SPAM’ is ook een Amerikaans merk van blikken vlees; hierover worden wel eens grappen gemaakt: zie ook http://www.spam.com/ [21].



23.6 Wat kan ik tegen SPAM doen?

Weinig. In sommige e-mailprogramma’s kunt u een lijst maken met ongewenste mailadressen. Dit biedt echter geen 100% oplossing, omdat veel ‘spammers’ niet-bestaande mailadressen gebruiken. Het e-mailsysteem van kennisnet biedt wel een mogelijkheid: het weigert berichten van niet-bestaande domeinnamen.

23.7 Wat is SPAM-relay?

SPAM-relay is het verzenden van SPAM-berichten via machines van andere organisaties. Zo verhullen ‘spammers’ hun identiteit, omdat het lijkt of het bericht van de desbetreffende organisatie afkomstig is. Zo voorkomen ‘spammers’ dat alle boze berichten bij hen terugkomen.

23.8 Wat kan worden gedaan tegen SPAM-relay?

De serversoftware voor e-mail van Netscape, die op de servers van kennisnet wordt gebruikt, en van Sendmail, het meest gebruikte mailprogramma, hebben functionaliteit om SPAM-relay tegen te gaan. Van elke inkomende verbinding wordt bekeken van welk IP-adres deze afkomstig is. Alleen computers binnen kennisnet mogen e-mail verzenden via deze server. Ook mag van buiten kennisnet alleen e-mail met een bestemming binnen kennisnet via deze server worden verzonden.

Deze functionaliteit is ook aanwezig bij veel andere serversoftware voor e-mail.

Een andere oplossing is ‘authenticated SMTP’, een uitbreiding op het protocol dat voor verzending van e-mail wordt gebruikt. Hierbij moet de gebruiker eerst een gebruikersnaam en een wachtwoord invoeren, voor hij zijn berichten kan verzenden. Deze optie wordt echter *niet* ondersteund door de mailservers van kennisnet.

23.9 Wat is een signature?

Een ‘signature’ is een soort handtekening die een gebruiker onder zijn e-mail- en nieuwsberichten kan plaatsen. Meestal vermeld de ‘signature’ de naam en enkele adresgegevens (e-mail, webpagina) van de afzender, maar sommige mensen maken er complete kunstwerken van. Op diverse websites worden verzamelingen van zulke ‘signatures’ bijgehouden. In Nederland zijn dat onder meer:

- http://huizen.dds.nl/~mwpieter/sigs[22]
- http://grid.let.rug.nl/~welling/sigs.html
- http://home.wxs.nl/~faase009/Signindex.html
- http://www.sci.kun.nl/thalia/funpage/koej/ascii-koej.html
- http://www.lstock.demon.nl/sigs.html

De term ‘signature’ wordt ook gebruikt voor een zogenoemde controlesom die voor een e-mailbericht kan worden berekend. Deze berekening wordt aangevuld met een geheime code. Vervolgens kan met een publieke code worden gecontroleerd of het bericht *echt* van een bepaalde persoon afkomstig is. Het bekendste programma hiervoor is PGP, voluit ‘Pretty Good Privacy’ (‘redelijk goede privacy’).

---

[21] Bron afbeelding: http://www.spam.com/.

[22] Deze verzameling is door medeauteur Menno Pieters aangelegd.

23.10 Ik krijg een waarschuwing om een bepaald e-mailbericht niet te openen. Wat moet ik doen?

Negeer zulke berichten. Vaak wordt verteld dat het openen van een bepaald e-mailbericht (bijvoorbeeld 'Penpal greetings') ervoor zorgt dat uw harde schijf wordt gewist. Dat kan *niet*. Een e-mail kan uw harde schijf niet wissen. Dergelijke berichten worden ook wel 'hoaxes' genoemd. Meer voorbeelden kunt u vinden op de volgende website:

http://ciac.llnl.gov/ciac/CIACHoaxes.html.

Let op!

Aanhangsels ('attachments') van e-mail kunnen wel gevaarlijk zijn voor uw systemen. Deze aanhangsels kunnen een virus of 'Trojaans Paard' bevatten. Scan aanhangsels altijd op virussen voor u ze opent. Virussen als 'Melissa' en 'I Love You' hebben bewezen dat ook bestanden van vrienden of collega's niet perse betrouwbaar zijn, omdat deze buiten hun medeweten kunnen zijn verzonden.

23.11 Kan ik mijn e-mail buiten kennisnet ophalen?

Ja. U moet dan zowel binnen als buiten het kennisnet gebruikmaken van dezelfde servernamen ('pop.kennisnet.nl' en 'imap.kennisnet.nl'). Dit geldt echter (nog) niet als u een eigen mailserver hebt.

23.12 Kan ik mijn e-mail buiten kennisnet verzenden?

Nee, dat kan niet via kennisnet. U kunt de mailservers van kennisnet alleen gebruiken om binnen kennisnet e-mail te verzenden. Als u bijvoorbeeld vanaf uw huisadres e-mail wilt verzenden, moet u de mailserver van uw lokale internetaanbieder gebruiken. U kunt als afzenderadres wel uw kennisnetadres gebruiken.

23.13 Als ik e-mail van buiten kennisnet probeer te verzenden, krijg ik een foutmelding

Als u e-mail van buiten kennisnet wilt verzenden en u werkt met Microsoft Outlook kunt u de volgende melding krijgen:



Figuur 223: Foutmelding bij verzenden e-mail van buiten kennisnet

Dit betekent dat u geen e-mail via deze server kunt verzenden. De server is beveiligd tegen 'SPAM-relay'; het doorsluizen van ongewenste e-mailberichten naar externe adressen. Alleen computers binnen kennisnet mogen e-mail buiten kennisnet verzenden via deze server. Ook mag van buiten kennisnet alleen e-mail met een bestemming binnen kennisnet via deze server worden verzonden.

Als u e-mail van buiten kennisnet wilt verzenden en u werkt met Netscape Communicator, wordt soms gevraagd om uw wachtwoord. Toch kunt u het bericht niet verzenden, omdat de mailserver niet werkt met 'authenticated SMTP' (zie ook paragraaf 23.8). Als u e-mail wilt verzenden buiten kennisnet, moet u gebruikmaken van de voorzieningen van uw lokale internetaanbieder.

23.14 Kan ik mijn externe e-mail binnen kennisnet ophalen?

Nee, dat is niet mogelijk met POP of IMAP. Als uw internetaanbieder het mogelijk maakt, kunt u uw e-mail laten doorsturen naar uw kennisnetadres. U kunt ook een speciale webmailsite gebruiken , zoals http://www.twigger.nl/, http://www.webmail.nl/ of http://www.xoip.nl/, of via een eventuele eigen webmailserver van uw aanbieder. Na het invoeren van de juiste gegevens, kunt u uw e-mail ophalen, lezen en beantwoorden.

24. Surfen op het internet (World Wide Web)

24.1 Wat zijn 'cookies'?

'Cookies' zijn kleine informatiebestanden die een website naar uw bladerprogramma kan sturen. Deze informatie kan worden gebruikt om bijvoorbeeld een boodschappenlijstje op te slaan in een elektronische winkel, maar ook om u toegang te verlenen tot delen van de website.

24.2 Zijn cookies gevaarlijk?

Nee. Wel kan met cookies worden vastgelegd hoe u door een website hebt gebladerd. Dit kan voor bepaalde aanbieders interessant zijn. Als zij deze gegevens aan uw naam en adresgegevens koppelen, kunnen zij dat gebruiken om u gericht reclame te sturen.

Cookies kunnen geen virussen bevatten en cookies bevatten alleen gegevens die door uzelf worden ingegeven. U kunt in uw bladerprogramma instellen dat cookies niet worden geaccepteerd of dat u eerst toestemming moet geven om een cookie te accepteren. Sommige websites vereisen echter het gebruik van cookies om bepaalde informatie te kunnen benaderen; in dat geval kunt u tijdelijk cookies accepteren.

24.3 Wat is Java?

Java is een programmeertaal. Deze taal wordt vooral toegepast voor programma's die op internet worden gebruikt. 'Java-applets' zijn kleine programma's die op een webpagina worden gebruikt om bepaalde functies uit te voeren, zoals een bewegend plaatje, een spelletjes of een kleine rekenmachine. Java is zo ontworpen, dat het niet uitmaakt op welk type computer en op welk besturingssysteem het wordt gebruikt.

24.4 Wat is JavaScript?

JavaScript is, net als Java, een programmeertaal. Met Java kunnen complete programma's worden gemaakt, terwijl met JavaScript alleen extra functionaliteit aan webpagina's kan worden toegevoegd. Vaak wordt JavaScript gebruikt om dynamische delen van een pagina te genereren, berekeningen te doen of formulieren te controleren voor verzending.

24.5 Wat is ActiveX?

ActiveX is een programmeertaal die is ontwikkeld door Microsoft. Net als met Java kunnen met ActiveX kleine programma's worden geschreven, die extra functionaliteit toevoegen aan webpagina's. Een belangrijk verschil is dat alleen bladerprogramma's die onder Windows werken, met ActiveX-componenten kunnen werken.

24.6 Wat zijn 'plug-ins'?

'Plug-ins' zijn hulpprogramma's die uw bladerprogramma nodig heeft om met bepaalde gegevens om te gaan, zodat u bijvoorbeeld filmpjes kunt bekijken, geluiden kunt beluisteren, speciale documenten kunt bekijken, enzovoort. In tegenstelling tot een Java-applet kan een plug-in niet op elk type computer of met elk besturingssysteem werken; voor ieder 'platform' is een aparte plug-in nodig.

24.7 Ik wil iets zoeken op het internet. Waar kan ik dat doen?

Op internet zijn diverse zoekmachines ('search engines') waarmee u op basis van een of meer trefwoorden kunt zoeken naar documenten, afbeeldingen en geluiden. Sommige zoekmachines zoeken alleen in Nederland, andere machine zoeken (ook) wereldwijd. Hieronder staat een aantal bekende zoekmachines.

Naam	Internet-adres	Wat?	Waar?
Altavista	http://www.altavista.com	Documenten	Wereldwijd

Naam	**Internet-adres**	**Wat?**	**Waar?**
Altavista Photo Finder	http://image.altavista.com	Afbeeldingen	Wereldwijd
DejaNews	http://www.dejanews.com	Nieuwsberichten	Wereldwijd
Excite	http://www.excite.com	Documenten	Wereldwijd
Google	http://www.google.com	Documenten	Wereldwijd
ILSE	http://www.ilse.nl	Documenten	Nederland
Lycos	http://www.lycos.com	Documenten	Wereldwijd
Lycos Pictures and Sounds	http://www.lycos.com/picturethis/	Afbeeldingen en geluiden	Wereldwijd
Track	http://www.track.nl	Documenten	Nederland
Yahoo*!*	http://www.yahoo.com	Documenten	Wereldwijd
Vinden	http://www.vinden.nl	Documenten	Wereldwijd
Vindex	http://www.vindex.nl	Documenten	Nederland
Zoek.NL	http://www.zoek.nl	Documenten	Nederland

Er zijn ook zogenoemde 'agents', die voor u verschillende zoekmachines kunnen raadplegen en met een meer afgewogen resultaat komen. Een voorbeeld is 'Copernic' (voor Windows), waarvan zowel een gratis versie als een uitgebreidere versie bestaat (zie deel III). Copernic kunt u ophalen vanaf de website http://www.copernic.com/.

24.8 Kan ik Secure Sockets Layer (SSL) gebruiken?

Secure Sockets Layer (SSL) wordt vaak gebruikt voor online bankieren en winkelen, en voor andere zaken waarbij een hoge mate van privacy is gewenst. De proxy-servers van kennisnet ondersteunen SSL voor HTTP (HTTPS) op dezelfde manier als zij normaal webverkeer (HTTP) ondersteunen.

25. Etiquette op het internet en kennisnet

25.1 Wat is ‘Netiquette’?

‘Netiquette’ is een verzameling van gedragsregels (etiquette) voor de omgang op internet met andere gebruikers. De ‘Netiquette’ beschrijft hoe gebruikers van het internet op een nette manier met elkaar kunnen communiceren. Zo wordt het bijvoorbeeld niet netjes geacht om een e-mailbericht of een nieuwsbericht geheel in hoofdletters te schrijven. Woorden geheel in hoofdletters schrijven, wordt opgevat als ‘schreeuwen’.

Ook wordt het niet gewaardeerd om berichten met een ellenlange ‘signature’ af te sluiten. Een ‘goede’ signature zou niet meer dan zo’n vier regels lang moeten zijn.

Uiteraard wordt het ook niet gewaardeerd wanneer men onheus wordt bejegend. Over het algemeen zijn de regels van ‘Netiquette’ vanzelfsprekend. Meer uitleg over de ‘Netiquette’ is te vinden op onderstaande website:

http://www.albion.com/netiquette/index.html.

25.2 Misbruik en klachten

Ondanks de ‘Netiquette’ komt het voor dat gebruikers van het internet zich niet gedragen zoals het hoort. Ook organisaties maken zich hieraan schuldig, bijvoorbeeld georganiseerde ‘spammers’ (zie ook paragraaf 23.5).

U kunt klachten indienen tegen afzenders van vervelende berichten. Als het gaat om georganiseerde spammers heeft dit weinig of geen zin, maar tegen een individu zijn de volgende maatregelen mogelijk:

- Klachten over e-mailberichten kunt u sturen naar ‘`postmaster@`*`domein`*’ of ‘`abuse@domein`’. Hierbij vervangt u *domein* door de desbetreffende domeinnaam.
- Klachten over de inhoud van een website kunt u sturen naar ‘webmaster@*domein*’. Hierbij vervangt u *domein* door de desbetreffende domeinnaam.

De desbetreffende misbruiker krijgt vervolgens meestal een waarschuwing. Bij aanhoudende klachten nemen de bevoegde personen ‘gepaste maatregelen’. Dit houdt meestal in dat de gebruiker de toegang tot de systemen wordt ontzegd en deze geen gebruik meer kan maken van het internet en andere diensten.

Bedenk wel dat het enige moeite en kennis van zaken vergt om met redelijke zekerheid te achterhalen waar een e-mailbericht werkelijk vandaan komt.

26. Problemen

In dit hoofdstuk worden enkele veelvoorkomende problemen behandeld.

26.1 Ik krijg geen IP-adres. Wat moet ik doen?

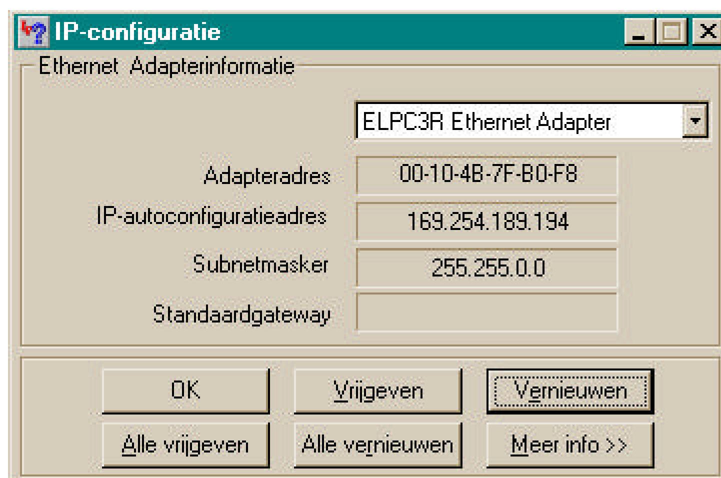
Als u geen IP-adres krijgt van de DHCP-server, is het mogelijk dat de DHCP-server niet functioneert of niet bereikbaar is. Wij raden u aan eerst de volgende zaken te controleren:

- Controleer of op beide aansluitingen van uw netwerk (dus op de hub, kabelmodem en/of router *en* op de computer) een lampje brandt. Dit is meestal een kleine groene LED. Als dat niet het geval is, kan de bekabeling defect zijn of is de verkeerde bekabeling gebruikt. Informatie over bekabeling vindt u in deel II.
- Controleer of op uw computer de juiste software en besturingssoftware is geïnstalleerd. Als u werkt met Windows 3.1x moet u wellicht een extra pakket (bijvoorbeeld Trumpet WinSock) installeren om gebruik te maken van TCP/IP. Als u werkt met Windows 95/98 moet u controleren of ondersteuning voor TCP/IP is geïnstalleerd en geconfigureerd (zie deel III). Als u werkt met Macintosh moet u controleren of MacTCP en bij voorkeur ook OpenTransport is geïnstalleerd en geconfigureerd (zie deel III).
- Probeer om 'met de hand' een IP-adres te krijgen.

  Windows 95/98

  Als u werkt met Windows 95/98, kunt u dit doen met het programma WinIPCfg. U start dit programma als volgt:

  - Klik op de knop 'Start'
  - Klik op de optie 'Uitvoeren' Er verschijnt een venster.
  - Typ in het venster de opdracht '`winipcfg`' en klik op de knop 'OK'.
  - Er verschijnt een venster.



Figuur 224: IP-configuratie

  - Selecteer in het invoervak met de keuzelijst uw 'ethernetadapter' (dus niet de PPP-adapter).
  - Klik op de knop 'Vrijgeven'.

- Klik vervolgens op de knop ‘Vernieuwen’. Nu moet binnen enkele seconden een IP-adres verschijnen. Als dat adres begint met ‘`169.254`’, is een fout opgetreden. Hier moet ‘`0.0.0.0`’ verschijnen, maar Microsoft heeft het ‘`169.254`’-netwerk gebruikt om zonder DHCP-server met computers onderling te kunnen communiceren.
- *Windows NT*

  Als u werkt met Windows NT, kunt u dit doen met het commando ‘IPCONFIG’. Dit doet u als volgt:

  - Klik op de knop ‘Start’.
  - Wijs de optie ‘Programma’s’ aan en klik op de optie ‘CMD’ of ‘MS-DOS-prompt’. Er verschijnt een CMD- of DOS-venster. Om een nieuw IP-adres te krijgen, moet u eerst het oude weggooien en daarna een nieuw adres aanvragen. Hierbij moet u de aanduiding van de netwerkaansluiting vermelden. Deze aanduiding ziet u als u het commando ‘`IPCONFIG`’ invoert *zonder* parameters. In het voorbeeld van Figuur 225, hieronder, is de aanduiding “`N1001`”.

    Om een nieuw IP-adres te krijgen moet u de volgende opdrachten uitvoeren:

    - Vrijgeven oud adres `IPCONFIG /RELEASE` *N0000*
    - Nieuw adres aanvragen `IPCONFIG /RENEW` *N0000*

    Hierbij staat *N0000* voor de aanduiding van de netwerkaansluiting.

    In Figuur 225 ziet u in een voorbeeld hoe u met ‘IPCONFIG’ een nieuw IP-adres kunt aanvragen.

```
Command Prompt

C:\>ipconfig /?

Windows NT IP Configuration

usage: ipconfig [/? | /all | /release [adapter] | /renew [adapter]]

       /?        Display this help message.
       /all      Display full configuration information.
       /release  Release the IP address for the specified adapter.
       /renew    Renew the IP address for the specified adapter.

The default is to display only the IP address, subnet mask and default gateway
for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

C:\>ipconfig /release N1001

Windows NT IP Configuration

IP address 10.17.42.12 successfully released for adapter "N1001"

C:\>ipconfig /renew N1001_
```

Figuur 225: Command Prompt, IPCONFIG

- *Apple Macintosh*

  Als u werkt met Apple Macintosh, kunt u dit als volgt doen:

  - Open het regelpaneel ‘TCP/IP’.
  - Activeer een andere configuratie.
  - Schakel terug naar de configuratie die DHCP gebruikt.

  Een andere manier die vaak werkt, is om de Macintosh in ‘sluimerstand’ te zetten via het menu of met de toetsencombinatie ‘Command-Shift-0 [= nul]’ en weer ‘wakker’ te maken met een willekeurige toetsaanslag.

Let op!
Als u bovenstaande controles hebt uitgevoerd, en het toch niet lukt om een geldig IP-adres te krijgen, kunt u bellen met het Servicepunt Kennisnet (zie Bijlage A, hoofdstuk 28).

26.2 Ik kan de webserver van kennisnet niet bereiken. Wat moet ik doen?

Als u de webserver van kennisnet niet kunt bereiken, gaat u als volgt te werk:

- Controleer of uw besturingssysteem en uw bladerprogramma de juiste TCP/IP-instellingen hebben, zoals beschreven in deel III.
- Controleer of u een geldig IP-adres krijgt.
- Controleer of u de proxy-servers kunt bereiken door het uitvoeren van een 'ping'[23] naar '`proxy.kennisnet.nl`'. Als de proxy-server bereikbaar is, moet u op internet kunnen en dus naar http://www.kennisnet.nl/.

Als u de webserver van kennisnet toch niet kunt bereiken, kunt u een storing melden bij het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zorg dat u alle gegevens bij de hand hebt en zoveel mogelijk details van de storing kunt melden.

26.3 Als ik met Telnet of FTP mijn server probeer te bereiken, duurt het heel lang voordat deze reageert. Wat moet ik doen?

Als u een Unix-achtig systeem gebruikt, zoals Solaris, FreeBSD of Linux, kan dit probleem zich voordoen. De serversoftware op deze systemen wil de naam van de desbetreffende computer vinden via de DNS-server. Zolang er nog private IP-adressen worden gebruikt, bestaat er binnen kennisnet nog geen DNS voor de computersystemen op de scholen. Hierdoor kan de DNS-server geen naam bij het desbetreffende IP-adres vinden. Na een bepaalde tijd zal deze het zoeken opgeven en kunt u alsnog gebruikmaken van Telnet of FTP.

Als (tijdelijke) oplossing kunt u een bestand op de server plaatsen met de naam `/etc/hosts`. Hierin vermeldt u de IP-adressen en namen van de werkplekken. Het bestand heeft de volgende opmaak:

- een IP-adres;
- een aantal spaties of een tab;
- een lange naam inclusief domein;
- een aantal spaties of een tab;
- een korte naam zonder domeinnaam.

Neem voor iedere werkplek een unieke naam op, bijvoorbeeld uw BRIN- en vestigingsnummer en een nummer voor de werkplek. Hieronder volgt een voorbeeld.

```
10.1.2.1      99ZZ00-0001.kennisnet.nl   99ZZ00-0001
10.1.2.2      99ZZ00-0002.kennisnet.nl   99ZZ00-0002
10.1.2.3      99ZZ00-0003.kennisnet.nl   99ZZ00-0003
10.1.2.4      99ZZ00-0004.kennisnet.nl   99ZZ00-0004
10.1.2.5      99ZZ00-0005.kennisnet.nl   99ZZ00-0005
...
```

Figuur 226: IP-adressen en namen van werkplekken

[23] Er zijn diverse gratis hulpmiddelen te krijgen, bijvoorbeeld 'NetLab' voor Windows, dat u via http://tucows.a2000.nl/ of http://www.tucows.com/ kunt vinden, of OTTool voor de Macintosh.

26.4 Ondersteunt Novell BorderManager meerdere C-klassen (blokken van 256 IP-adressen)?

Nee. Novell BorderManager kan uitsluitend met gehele C-klassen overweg. Novell heeft wel aangekondigd op korte termijn ‘supernetting’ (meerdere blokken van 256 IP-adressen) te zullen ondersteunen.

26.5 Ik kan het internet niet bereiken. Wat moet ik doen?

Als u het internet niet kunt bereiken, moet u eerst controleren of de desbetreffende proxy-server juist is ingesteld (zie deel III). U kunt namelijk voor geen enkele dienst *rechtstreeks* een verbinding maken naar systemen buiten het kennisnet.

Als u de instellingen hebt gecontroleerd en u toch internet niet kunt bereiken, neemt u contact op met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Noteer exact de melding die u krijgt van uw programma.

Let op!

U kunt in dit geval niet met een ‘ping’ controleren of systemen buiten kennisnet bereikbaar zijn. In principe wordt al het verkeer tussen kennisnet en het internet geblokkeerd, met enkele speciale uitzonderingen voor de servers van kennisnet zelf.

26.6 Hoe kan ik mijn verbinding testen op snelheid?

Het is erg moeilijk om met zekerheid de snelheid van een verbinding te bepalen. Er zijn diverse meetmethoden, maar deze geven vaak uiteenlopende resultaten. Het testen van de netwerksnelheid met FTP is geen goede oplossing want:

- het ene FTP-programma is logger (en trager) dan het andere;
- de implementatie van TCP/IP in een besturingssysteem kan te wensen overlaten;
- de locatie waarvandaan het bestand komt, is ook een factor die het resultaat negatief kan beïnvloeden, want:
    - de server kan het erg druk hebben,
    - de verbinding van de desbetreffende server met het internet kan traag zijn;
- de snelheidsindicatie van FTP-software is niet altijd eenduidig. Netwerksnelheden worden meestal uitgedrukt in kilobits of megabits per seconde (kb/s of Mb/s, met kleine letter b). De snelheidsindicatie van FTP-software wordt vaak uitgedrukt in kilo*bytes* of mega*bytes* per seconde (kB/s of MB/s, met hoofdletter B). Dat scheelt een factor acht. Doordat niet alle programma’s correct hoofd- en kleine letters weergeven, kan de snelheid te laag lijken.

Ongeveer dezelfde argumenten gelden voor HTTP. Bovendien wordt informatie via HTTP vaak zo gecodeerd, dat ongeveer anderhalf keer zoveel data worden verzonden als uiteindelijk op uw harde schijf belanden.

Als u vermoedt dat uw verbinding te traag is, kunt u contact opnemen met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zij kunnen een indicatieve meting laten uitvoeren. Als daar aanleiding voor is, kan op locatie een specifieke en exactere meting van uw aansluiting worden uitgevoerd.

Overigens wordt er al bij het aansluiten van uw schoolnetwerk op kennisnet een meting van de capaciteit uitgevoerd. Als daaruit blijkt dat de aansluiting niet voldoende presteert, worden maatregelen genomen.

26.7 Waarom is kennisnet op sommige momenten traag?

De traagheid van kennisnet wordt voor een groot deel bepaald door het systeem waarmee u een verbinding maakt. Als het systeem in Amerika staat, wordt de verbinding trager naarmate de dag vordert. Het dagelijks leven in Amerika komt, afhankelijk van de tijdzone, zo'n zes tot tien uur later op gang dan in Europa. Verbindingen met het Verre Oosten (onder andere Japan en Taiwan) lopen vaak via Amerika en zijn daardoor soms ook langzaam. Kennisnet kan daar niets aan doen. Over het algemeen is het netwerk van kennisnet zelf niet de remmende factor. Het netwerk biedt voldoende capaciteit. Deze wordt voortdurend gecontroleerd om te zorgen dat tijdig extra capaciteit kan worden ingeschakeld. Wel kunnen de proxy-servers bij zeer zware belasting minder snel reageren.

26.8 Waar kan ik een probleem melden?

Als u een probleem hebt bij het gebruik van kennisnet, kunt u contact opnemen met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zij kunnen u meestal helpen. Ook voor problemen met het landelijke of kabelnetwerk van kennisnet, of problemen met de diensten van kennisnet, kunt u contact opnemen met het Servicepunt Kennisnet.

Let op!

Verzamel zoveel mogelijk informatie over het probleem, zodat goed duidelijk wordt waar en wanneer de problemen optreden.

26.9 Worden werkzaamheden aan kennisnet gemeld aan scholen?

Het is gebruikelijk dat grote werkzaamheden minimaal een week voordat deze worden uitgevoerd, via de website van kennisnet (http://www.kennisnet.nl/) worden aangekondigd. Zo kunt u rekening houden met deze werkzaamheden. Soms wordt tevens op basis van een e-maillijst een bericht verzonden. Het is niet altijd mogelijk om elke school een persoonlijke brief en/of fax te sturen.

27. Aanvullende diensten

27.1 Hoe krijg ik een (extra) aansluiting op kennisnet?

Als u een (extra) aansluiting op kennisnet wilt, neemt u contact op met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zij kunnen u precies vertellen hoe en waar u uw verzoek moet indienen.

27.2 Hoe kan ik mijn aansluiting opzeggen?

Als u uw aansluiting op kennisnet wilt opzeggen, neemt u contact op met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zij kunnen u precies vertellen hoe en waar u uw verzoek moet indienen.

27.3 Wat moet ik doen als onze school gaat verhuizen?

Als uw school gaat verhuizen, moet u dat ruimschoots van tevoren melden bij het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zij sturen u een formulier waarop u de wijzigingen kunt aangeven (nieuw adres of nieuwe adressen, ander aantal werkplekken, enzovoort). Vervolgens worden de benodigde maatregels genomen, aangezien u wellicht in het verzorgingsgebied van een andere kabelmaatschappij komt. Bovendien is het waarschijnlijk dat uw IP-adressen zullen veranderen. Als uw school fuseert of een aantal vestigingen samengaat, is de operatie mogelijk nog ingrijpender.

27.4 Hoe kan ik mijn aansluiting of de gebruikte diensten wijzigen?

Als u uw aansluiting of de gebruikte diensten wilt wijzigen, neemt u contact op met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Zij sturen u een formulier waarop u uw wensen kenbaar kunt maken. Vervolgens nemen zij contact met u op om uw wensen te bespreken. Standaarddiensten worden vrij snel gerealiseerd. Als u zeer speciale wensen hebt, kan het langer duren.

27.5 Waar kan ik aanvragen om mijn IP-reeks te vergroten of te verkleinen?

U kunt een e-mailbericht sturen aan servicedesk@nltree.nl of bellen met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28).

27.6 Ik wil meer routerpoorten openstellen. Wat moet ik doen?

Controleer op basis van de gegevens in deel I of u met het bestaande beveiligingsfilter kunt werken. Poorten 1024 en hoger staan bijna allemaal open voor werkstations. Voor een deel van uw IP-reeks staan bijna alle poorten (behalve zeer kwetsbare poorten) open om diensten aan te bieden.

Als de instellingen van uw router toch moeten worden gewijzigd, moet u per fax een verzoek zenden aan nl.tree: faxnummer (070) 89 000 99. Het verzoek wordt door het Ministerie van Onderwijs, Cultuur en Wetenschappen beoordeeld. Zij nemen contact op met uw instelling en stellen een contract op. Als het getekende contract is geretourneerd, wordt de technische realisatie in gang gezet.

27.7 Kan ik meer mailadressen/postbussen krijgen?

Als bij uw instelling een tekort aan mailadressen/postbussen dreigt, bijvoorbeeld doordat uw school qua leerlingenaantal snel groeit, kunt u extra mailadressen laten aanmaken. Hiertoe moet u een aanvraag indienen bij het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Geef hierbij aan waarom u extra mailadressen/postbussen nodig hebt en hoeveel u er wilt laten bijmaken.

27.8 Hoe kan ik een eigen domeinnaam aanvragen?

Als u een eigen domeinnaam wilt aanvragen, neemt u contact op met het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Het Servicepunt Kennisnet heeft een formulier beschikbaar voor het aanvragen van domeinnamen voor e-mail en/of voor webservices. Het Servicepunt dient vervolgens een verzoek in bij de Stichting Internet Domeinregistratie Nederland (IDNL). Zij controleren of de door u gewenste domeinnaam niet strijdig is met de reglementen en of is voldaan aan bepaalde voorwaarden. Als alles in orde is wordt het domein, tegen betaling, aan u toegewezen. Vervolgens zal kennisnet de diensten verlenen om uw domein in werking te stellen, zoals DNS en dergelijke.

Meer informatie over dit onderwerp kunt u vinden op de website van de Stichting Internet Domeinregistratie Nederland: http://www.domain-registry.nl/. Hier vindt u onder andere het reglement, waarin wordt vermeld aan welke eisen een domeinnaam moet voldoen en wat niet mag. Er is ook een uitputtende lijst beschikbaar van domeinnamen die reeds zijn geweigerd of gereserveerd.

Let op!

De aanvraag van een domeinnaam brengt kosten met zich mee: eenmalig voor de aanvraag en jaarlijks voor het behoud ervan.

27.9 Onze school heeft een eigen domeinnaam. Kan kennisnet deze overnemen?

Dat is mogelijk, maar alleen als *u* de eigenaar bent van de domeinnaam en niet uw internetaanbieder. Maar ook als *u* de eigenaar bent van de domeinnaam, is medewerking van uw huidige aanbieder wel vereist.

U moet een verzoek indienen bij het Servicepunt Kennisnet (zie bijlage A, hoofdstuk 28). Vermeld in dat verzoek alle gegevens over de domeinnaam. Als u uw domein gebruikt voor meer dan een webserver en een bestemming voor uw mail, stuur dan een uitdraai van de ‘zone-informatie’ met uw verzoek mee.

27.10 Kan ik een Virtual Private Network (VPN) opzetten binnen kennisnet?

Dat is mogelijk. Op dit moment werkt kennisnet aan een standaardoplossing voor veilige verbindingen tussen schoollocaties. Deze oplossing wordt momenteel uitgeprobeerd tussen een aantal schoollocaties. Behalve de standaardoplossing kunt u ervoor kiezen om een eigen VPN-oplossing te realiseren.

Houd ermee rekening dat u mogelijk een snellere verbinding moet aanvragen om de vereiste capaciteit te kunnen garanderen. Veel verbindingen binnen kennisnet zijn bovendien asymmetrisch. Dat wil zeggen, dat de capaciteit van kennisnet naar uw instelling hoger is dan vice versa. Voor een VPN heeft u waarschijnlijk behoefte aan een symmetrische verbinding.

28. Bijlage A: Belangrijke adressen en telefoonnummers

28.1 Servicepunt Kennisnet (SPK)

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt Kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op het nummer 0800-KENNISNET (0800-536647638). Zie ook deel 0.

28.2 Handboek Kennisnet

Voor op- of aanmerkingen en aanvullingen voor het 'Handboek kennisnet' kunt u e-mail sturen naar handboek@kennisnet.nl.

29. Bijlage B: Squid

U kunt niet zonder meer een eigen proxy-server installeren; deze proxy-server moet op zijn beurt gebruikmaken van de proxy-servers van kennisnet. Om uw proxy-server te koppelen aan de proxy-server van kennisnet, kunt u gebruikmaken van het programma 'Squid'.



In het configuratiebestand van Squid (`squid.conf`) moet u instellen dat uw proxy-server gebruik maakt van de proxy-server van kennisnet.

Van Squid zijn twee werkende configuratievoorbeelden beschikbaar: één voor versie 1.2.x en één voor 2.2.x. De relevante gedeelten worden in deze bijlage weergegeven. In het standaard meegeleverde voorbeeld kunt u deze stukken eenvoudig terugvinden en aan de hier gegeven voorbeelden aanpassen. U kunt Squid ophalen van http://www.squid-cache.org/.

29.1 Squid 1.2.x

29.1.1 Parents

Eerst moet u de zogenaamde 'parent hosts' definiëren. Dit zijn de machines waaraan uw proxy-server kan refereren om gegevens op te vragen, die zich niet in de lokale buffer ('cache') bevinden of waarvan de geldigheid is verlopen.

```
cache_host proxy.kennisnet.nl parent 8080 3130 no-query
```

29.1.2 Domeingrenzen (versie 1.x.x)

U moet de gegevens inperken die in de buffers worden opgenomen. U kunt dit het beste doen op basis van de domeinnaam. De inperking van het te bufferen domein kunt u controleren met het commando 'inside_firewall':

```
inside_firewall kennisnet.nl
```

Met het commando 'local_domain' geeft u het lokale domein aan:

```
local_domain kennisnet.nl
```

29.2 Squid 2.2.x

29.2.1 Parents cache proxy

Eerst moet u de 'parent cache proxy' voor Squid instellen. Vervolgens moet u instellen dat de proxy-server nooit direct verbinding zoekt met de desbetreffende hosts, maar dat de verbinding moet worden gemaakt via de proxy-server van kennisnet. Hiertoe voegt u de volgende regels toe aan uw configuratiebestand:

```
cache_peer proxy.kennisnet.nl parent 8080 3130 no-query default
acl all src 0.0.0.0/0.0.0.0
never_direct allow all
```

In principe is dit de enige aanpassing in het standaard-configuratiebestand van Squid die nodig is om gebruik te kunnen maken van een eigen proxy-server binnen kennisnet. Voor optimale prestaties moet u zelf wel nog bepalen hoeveel geheugen en schijfruimte Squid mag gebruiken.

29.2.2 Domeingrenzen (versie 2.x.x)[24]

Als u in deze versie de domeingrenzen wilt vastleggen, moet u weten dat in deze en nieuwere versies de commando's 'inside_firewall', 'local_domain', 'local_ip' en 'firewall_ip' niet meer beschikbaar zijn. In versie 2.0.0 en hoger wordt gebruik gemaakt van de commando's 'never_direct' en 'always_direct'. Verder moet in de zogenoemde ACL's (Access Control Lists) worden aangeven voor welke adressen de 'parents' gebruikt mogen worden.

Een compleet configuratievoorbeeld voor Squid versie 2.2 stable 5 vindt u in paragraaf 29.5.

29.3 Overige opties

Verdere opties zult u naar eigen inzicht moeten wijzigen. Deze hebben vooral betrekking op de buffergrootte, de afhandeling van verzoeken, logbestanden en beveiliging. Raadpleeg hiervoor de bijgevoegde documentatie of de documentatie op het internet: http://squid.nlanr.net/Squid/Users-Guide/.

29.4 Filters instellen

Als uw proxy-server daartoe in staat is (eventueel na installatie van de juiste software), kunt u zelf filters instellen om bepaalde informatie voor uw gebruikers te blokkeren. De wijze van filteren is afhankelijk van het product dat u gebruikt. Vaak kunt u een lijst met hetzij verboden, hetzij toegestane adressen opgeven. Bij sommige pakketten kunt u categorieën van adressen blokkeren of vrijgeven. Bij dergelijke systemen kunt u via de leverancier vaak een abonnement afsluiten om regelmatig nieuwe filterinformatie te ontvangen.

29.5 Voorbeeldconfiguratie Squid 2.2 stable 5

In deze bijlage staat een configuratie voor Squid versie 2.2 stable 5. Deze configuratie blijkt in de praktijk goed te werken. Hierbij wordt gebruik gemaakt van de proxy-servers van kennisnet. Iedereen mag dit bestand gebruiken, maar wel op eigen risico. De belangrijkste punten voor deze configuratie:

- Squid stuurt alle verzoeken door naar de proxy-server van kennisnet.
- Squid luistert op poort 8080.
- Squid heeft een geheugenbuffer van 8 MB (deze mag groter zijn).
- Squid zoekt alle benodigde bestanden in `/usr/local/squid/`.

  Let op!

  De exacte locatie verschilt per Unix-variant en -distributie.
- Squid zoekt geen DNS-informatie.
- De cache manager (`cachemgr.cgi`) kan worden gebruikt.

Verder raden wij aan om het systeem zo te optimaliseren, dat het geheugen effectief wordt gebruikt: gebruik wat u kunt missen. Ongeveer de helft tot driekwart van het fysiek aanwezige geheugen is waarschijnlijk een goede keuze. Zet bij voorkeur een machine speciaal als proxy-server in om de prestaties zo hoog mogelijk te houden.

```
# Generated automatically from squid.conf.pre.in by configure.
#
# $Id: squid.conf.pre.in,v 1.93.2.16 1998/05/01 23:21:03 wessels Exp $
#

#  TAG: http_port
#       The port number where squid will listen for HTTP client
#       requests.  Default is 3128, for httpd-accel mode use port 80.
#       May be overridden with -a on the command line.
#
http_port 8080
```

[24] Met dank aan Jeroen Oldenhof, systeembeheerder Drenthecollege.

```
#  TAG: icp_port
#       The port number where squid send and receive ICP requests to
#       and from neighbor caches.  Default is 3130.  To disable use
#       "0".  May be overridden with -u on the command line.
#
icp_port 0
#  TAG: mcast_groups
#       This tag specifies a list of multicast groups which your
#       server should join to receive multicasted ICP requests.
#
#       NOTE!  Be very careful what you put here!  Be sure you
#       understand the difference between an ICP query and an ICP
#       reply.  This option is to be set only if you want to RECEIVE
#       multicast queries.  Do NOT set this option to SEND multicast
#       ICP (use cache_host for that).  ICP replies are always sent via
#       unicast, so this option does not affect whether or not you will
#       receive replies from multicast group members.
#
#       You must be very careful to NOT use a multicast address which
#       is already in use by another group of caches.  NLANR has been
#       assigned a block of multicast address space for use in Web
#       Caching.  Plese write to us at nlanr-cache@nlanr.net to receive
#       an address for your own use.
#
#       Usage:  mcast_groups 239.128.16.128 224.0.1.20
#
#       By default, squid doesn't listen on any multicast groups.
#
#mcast_groups 239.128.16.128
#  TAG: tcp_incoming_address
#  TAG: tcp_outgoing_address
#  TAG: udp_incoming_address
#  TAG: udp_outgoing_address
#
#       Usage: tcp_incoming_address 10.20.30.40
#              udp_outgoing_address fully.qualified.domain.name
#
#       These tags have replaced 'bind_address' and 'outbound_address'
#       to provide more control for multihomed hosts.
#
#       tcp_incoming_address    is used for the HTTP socket which accepts
#                               connections from clients and other caches.
#       tcp_outgoing_address    is used for connections made to remote
#                               servers and other caches.
#       udp_incoming_address    is used for the ICP socket receiving packets
#                               from other caches.
#       udp_outgoing_address    is used for ICP packets sent out to other
#                               caches.
#
#       The defaults behaviour is to not bind to any specific address.
#
#       NOTE, udp_incoming_address and udp_outgoing_address can not have
#       the same value since they both use port 3130.
#
#tcp_incoming_address 0.0.0.0
#tcp_outgoing_address 0.0.0.0
#udp_incoming_address 0.0.0.0
#udp_outgoing_address 0.0.0.0

# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
#-----------------------------------------------------------------------------
--

#  TAG: cache_host
```

```
#       To specify other caches in a hierarchy, use the format:
#
#           hostname type http_port icp_port
#
#   For example,
#
#       #                                         proxy  icp
#       #           hostname             type     port   port  options
#       #           -------------------- -------- ----- ----- -----------
#       cache_host bigserver.usc.edu     parent    3128  3130  [proxy-only]
#       cache_host littleguy1.usc.edu    sibling   3128  3130  [proxy-only]
#       cache_host littleguy1.usc.edu    sibling   3128  3130  [proxy-only]
#
#             type:  either 'parent', 'sibling', or 'multicast'.
#
#       proxy_port:  The port number where the cache listens for proxy
#                    requests.
#
#         icp_port:  Used for querying neighbor caches about
#                    objects.  To have a non-ICP neighbor
#                    specify '7' for the ICP port and make sure the
#                    neighbor machine has the UDP echo port
#                    enabled in its /etc/inetd.conf file.
#
#          options: proxy-only
#                   weight=n
#                   ttl=n
#                   no-query
#                   default
#                   round-robin
#                   multicast-responder
#
#                   use 'proxy-only' to specify that objects fetched
#                   from this cache should not be saved locally.
#
#                   use 'weight=n' to specify a weighted parent.
#                   The weight must be an integer.  The default weight
#                   is 1, larger weights are favored more.
#
#                   use 'ttl=n' to specify a IP multicast TTL to use
#                   when sending an ICP request to this address.
#                   Only useful when sending to a multicast group.
#                   Because we don't accept ICP replies from random
#                   hosts, you must configure other group members as
#                   peers with the 'multicast-responder' option below.
#
#                   use 'no-query' to NOT send ICP queries to this
#                   neighbor.
#
#                   use 'default' if this is a parent cache which can
#                   be used as a "last-resort." You should probably
#                   only use 'default' in situations where you cannot
#                   use ICP with your parent cache(s).
#
#                   use 'round-robin' to define a set of parents which
#                   should be used in a round-robin fashion in the
#                   absence of any ICP queries.
#
#                   'multicast-responder' indicates that the named peer
#                   is a member of a multicast group.  ICP queries will
#                   not be sent directly to the peer, but ICP replies
#                   will be accepted from it.
#
#       NOTE: non-ICP neighbors must be specified as 'parent'.
```

```
#
#cache_host hostname type 3128 3130
#  TAG: cache_host_domain
#       Use to limit the domains for which a neighbor cache will be queried.
#       Usage:
#
#       cache_host_domain cache-host domain [domain ...]
#       cache_host_domain cache-host !domain
#
#       For example, specifying
#
#               cache_host_domain bigserver.usc.edu     .edu
#
#       has the effect such that UDP query packets are sent to
#       'bigserver' only when the requested object exists on a
#       server in the .edu domain.  Prefixing the domainname
#       with '!' means that the cache will be queried for objects
#       NOT in that domain.
#
#       NOTE:   * Any number of domains may be given for a cache-host,
#                 either on the same or separate lines.
#               * When multiple domains are given for a particular
#                 cache-host, the first matched domain is applied.
#               * Cache hosts with no domain restrictions are queried
#                 for all requests.
#               * There are no defaults.
#               * There is also a 'cache_host_acl' tag in the ACL
#                 section.

#  TAG: neighbor_type_domain
#
#       usage: neighbor_type_domain parent|sibling domain domain ...
#
#       Modifying the neighbor type for specific domains is now
#       possible.  You can treat some domains differently than the the
#       default neighbor type specified on the 'cache_host' line.
#       Normally it should only be necessary to list domains which
#       should be treated differently because the default neighbor type
#       applies for hostnames which do not match domains listed here.
#
#EXAMPLE:
#       cache_host  parent cache.foo.org 3128 3130
#       neighbor_type_domain cache.foo.org sibling .com .net
#       neighbor_type_domain cache.foo.org sibling .au .de

#  TAG: inside_firewall
#       This tag specifies a list of domains inside your internet
#       firewall.
#
#       Usage: inside_firewall my.domain  [ my.other.domain ...]
#              !out.my.domain my.domain
#
#       The use of this tag affects the server selection algorithm in
#       two ways.  Objects which do not match any of the listed domains
#       will be considered "beyond the firewall."  For these:
#               - There will be no DNS lookups for the URL-host.
#               - The object will always be fetched from one of
#                 the parent or neighbor caches.
#
#       As a special case you may specify the domain as 'none' to force
#       all requests to be fetched from neghbors and parents.
#       Prefixing a domain name with '!' means the domain is NOT inside
#       your firewall.
#
```

```
#inside_firewall topsecret.com
#inside_firewall kennisnet.nl
cache_peer proxy.kennisnet.nl parent 8080 3130 no-query default
acl all src 0.0.0.0/0.0.0.0
never_direct allow all

#  TAG: local_domain
#       This tag specifies a list of domains local to your organization.
#
#       Usage: local_domain my.domain [ my.other.domain ...]
#
#       For URLs which are in one of the local domains, the object
#       is always fetched directly from the source and never from a
#       neighbor or parent.
#
#local_domain ce.nihon-u.ac.jp
#  TAG: local_ip
#       This tag specifies a list of network addresses local to your
#       organization.
#
#       Usage: local_ip ip-address
#
#       This tag is similar to local_domain, except that the IP-address
#       of the URL-host is checked.  This requires that a DNS lookup
#       be done on the URL-host.  For this reason, local_domain is
#       preferred over local_ip.  By using local_domain it may be
#       possible to avoid the DNS lookup altogether and deliver the
#       object with less delay.
#
#local_ip 10.0.0.0
#local_ip 192.168.0.1

#  TAG: firewall_ip
#
#       Just like 'inside_firewall' but for IP addresses.  NOTE:
#       firewall_ip and local_ip are mutually exclusive.  If you
#       use firewall_ip then local_ip will be ignored.
#
#firewall_ip 10.0.0.0
#firewall_ip 172.16.0.0
#  TAG: single_parent_bypass
#       This tag specifies that it is okay to bypass the hierarchy
#       "Pinging" when there is only a single parent for a given URL.
#
#       Usage: single_parent_bypass on|off
#
#       Before actually sending ICP "ping" packets to parents and
#       neighbors, we figure out which hosts would be pinged based
#       on the cache_host_domain rules, etc.  Often it may be the
#       case that only a single parent cache would be pinged.
#
#       Since there is only a single parent, there is a very good
#       chance that we will end up fetching the object from that
#       parent.  For this reason, it may be beneficial to avoid
#       the ping and just fetch the object anyway.
#
#       However, if we avoid the ping, we will be assuming that the
#       parent host is reachable and that the cache process is running.
#       By using the ping, we can be reasonably sure that the parent
#       host will be able to handle our request.  If the ping fails then
#       it may be possible to fetch the object directly from the source.
#
#       To favor the resiliency provided by the ping algorithm,
#       single_parent_bypass is 'off' by default.
```

```
#
#single_parent_bypass off
#  TAG: source_ping
#       If source_ping is enabled, then squid will include the source
#       provider site in its selection algorithm.  This is accomplished
#       by sending ICP "HIT" packets to the UDP echo port of the source
#       host.  Note that using source_ping may send a fair amount of UDP
#       traffic out on the internet and may irritate paranoid network
#       administrators.
#
#       Note that source_ping is incompatible with inside_firewall.
#       For hosts beyond the firewall, source_ping packets will never
#       be sent.
#
#       By default, source_ping is off.
#
#source_ping off
#  TAG: neighbor_timeout (seconds)
#       This controls how long to wait for replies from neighbor caches.
#       If none of the parent or neighbor caches reply before this many
#       seconds (due to dropped packets or slow links), then the object
#       request will be satisfied from the default source.  The default
#       timeout is two seconds.
#
#neighbor_timeout 2
#  TAG: hierarchy_stoplist
#       A list of words which, if found in a URL, cause the object to
#       be handled directly by this cache.  In other words, use this
#       to not query neighbor caches for certain objects.  You may
#       list this option multiple times.
#
#       The default is to directly fetch URLs containing 'cgi-bin' or '?'.
#
hierarchy_stoplist cgi-bin ?
#  TAG: cache_stoplist
#       A list of words which, if found in a URL, cause the object to
#       immediately removed from the cache.  In other words, use this
#       to force certain objects to never be cached.  You may list this
#       option multiple times.
#
#       The default is to not cache URLs containing 'cgi-bin' or '?'.
#
#cache_stoplist cgi-bin ?
#  TAG: cache_stoplist_pattern          # case sensitive
#  TAG: cache_stoplist_pattern/i        # case insensitive
#
#       Just like 'cache_stoplist' but you can use regular expressions
#       instead of simple string matching.  There is no default.
#
#cache_stoplist_pattern
#  TAG: no_cache
#
#       Use ACL elements to specify uncachable objects.  For example,
#       this prevents caching of objects downloaded from servers whose
#       IP addresses are in the 192.172.226.0 network:
#
#       acl FOO dst 192.172.226.0/24
#       no_cache deny FOO
#
#       You MUST use the 'deny' keyword before the list of ACL names.
#       For more details on how to specify ACLs and access lists,
#       See the comments for 'http_access' below, and please read the
#       Squid FAQ (http://squid.nlanr.net/Squid/FAQ/FAQ.html).
#
```

```
# OPTIONS WHICH AFFECT THE CACHE SIZE
#-----------------------------------------------------------------------------
--

#
#  TAG: cache_mem (megabytes)
#       Maximum amout of VM used to store objects in memory.
#       This includes:
#               in-transit objects,
#               negative-cached objects,
#               “hot” objects
#       The value of cache_mem is an upper limit on the size of the
#       “in-memory object data” pool.  This is a pool of 4k pages used
#       to hold object data.
#
#       In-transit objects have priority over the others.  When
#       additional space is needed for incoming data, negative-cached
#       and hot objects will be released.  In other words, the
#       negative-cached and hot objects will fill up any unused space
#       not needed for in-transit objects.
#
#       The values of cache_mem_low and cache_mem_high (below) can be
#       used to tune the use of the memory pool.  When the high mark is
#       reached, in-transit and hot objects will be released to clear
#       space.  When an object transfer is completed, it will remain in
#       memory only if the current memory usage is below the low water
#       mark.
#
#       The default is 8 Megabytes.
#
cache_mem  8 MB
#  TAG: cache_swap (megabytes)
#       Maximum about of disk space used by the cache.  The default is
#       100 megabytes.  When the disk usage gets to this size, the cache
#       uses LRU replacement to evict objects as new objects are cached.
#       Note that cache_swap is set to:
#               max(cache_mem, cache_swap_specified)
#       to guard against users’ accidentally specifying a smaller
#       cache_swap than cache_mem size.
#
#cache_swap 100 MB

#  TAG: cache_swap_low  (percent, 0-100)
#  TAG: cache_swap_high (percent, 0-100)
#       The low- and high-water marks for cache LRU replacement.
#       LRU replacement begins when the high-water mark is reached
#       and ends when enough objects have been removed and the low-water
#       mark is reached. Defaults are 90% and 95%.
#
cache_swap_low  90
cache_swap_high 95

#  TAG: cache_mem_low  (percent, 0-100)
#  TAG: cache_mem_high (percent, 0-100)
#       The low- and high-water mark for cache memory storage.  When
#       the amount of RAM used by the hot-object RAM cache reaches this
#       point, the cache starts throwing objects out of the RAM cache
#       (but they remain on disk).  Defaults are 75% and 90%.
#
#cache_mem_low  75
#cache_mem_high 90

#  TAG: maximum_object_size
```

```
#       Objects larger than this size will NOT be saved on disk.  The
#       value is specified in kilobytes, and the default is 4MB.
#
#maximum_object_size 4096
#  TAG: ipcache_size (number of entries)
#  TAG: ipcache_low  (percent)
#  TAG: ipcache_high (percent)
#       The size, low-, and high-water marks for the IP cache.
#
ipcache_size 1024
ipcache_low  90
ipcache_high 95


# LOGFILE PATHNAMES AND CACHE DIRECTORIES
#-----------------------------------------------------------------------------
--

#  TAG: cache_dir
#       Directory for on-disk cache storage.  The cache will change into
#       this directory when running.  The default is
#       /usr/local/squid/cache.
#
#       You can specify multiple cache_dir lines to spread the
#       cache among different disk partitions.
#
cache_dir /usr/local/squid/cache 100 16 256
#  TAG: cache_access_log
#       Logs the client request activity.  Contains an entry for
#       every HTTP and ICP request received.
#
cache_access_log /usr/local/squid/logs/access.log
#  TAG: cache_log
#       Cache logging file.  Set logging levels with “debug_options” below.
#
cache_log /usr/local/squid/logs/cache.log
#  TAG: cache_store_log
#       Logs the activities of the storage manager.  Shows which
#       objects are ejected from the cache, and which objects are
#       saved and for how long.  To disable, enter “none”.
#
cache_store_log /usr/local/squid/logs/store.log
#  TAG: cache_swap_log
#       Location for the cache “swap log.”  This log file holds the
#       metadata of objects saved on disk.  It is used to rebuild the
#       cache during startup.  Normally this file resides in the first
#       ‘cache_dir’ directory, but you may specify an alternate
#       pathname here.  Note you must give a full filename, not just
#       a directory.
#
#cache_swap_log /usr/local/squid/cache
#  TAG: emulate_httpd_log
#       The Cache can emulate the log file format which many ‘httpd’
#       programs use.  To disable/enable this emulation, set
#       emulate_httpd_log to ‘off’ or ‘on’.  The default
#       is to use the native log format.
#
emulate_httpd_log off
#  TAG: log_mime_hdrs
#       The Cache can record both the request and the response
#       MIME headers for each HTTP transaction.  The headers are
#       encoded safely and will appear as two bracketed fields
#       at the end of the access log (for either the native
#       or httpd-emulated log formats).  To enable this logging
```

```
#       set log_mime_hdrs to 'on'.
#
#       NOTE: support for this may require you to define
#       LOG_FULL_HEADERS before compiling.
#
#log_mime_hdrs off
#  TAG: useragent_log
#       If compiled with "-DUSE_USERAGENT_LOG=1" Squid will write
#       the User-Agent field from HTTP requests to the filename
#       specified here.  By default useragent_log is disabled.
#
#useragent_log none
#  TAG: pid_filename
#       A pathname to write the process-id to.  To disable, enter "none".
#
pid_filename /usr/local/squid/logs/squid.pid
#  TAG: debug_options
#       Logging options are set as section,level where each source file
#       is assigned a unique section.  Lower levels result in less
#       output,  Full debugging (level 9) can result in a very large
#       log file, so be careful.  The magic word "ALL" sets debugging
#       levels for all sections.  We recommend normally running with
#       "ALL,1".
#
#debug_options ALL,1
#  TAG: ident_lookup
#       If you wish to make an RFC931/ident lookup of the client username
#       for each connection, enable this.  It is off by default.
#
#ident_lookup off
#  TAG: log_fqdn
#       Turn this on if you wish to log fully qualified domain names
#       in the access.log.
#
log_fqdn off
#  TAG: client_netmask
#       A netmask for client addresses in logfiles and cachemgr output.
#       Change this to protect the privacy of your cache clients.
#
#client_netmask 255.255.255.0

# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
#-----------------------------------------------------------------------------
--

#  TAG: ftpget_program
#       Where to find the 'ftpget' program that retrieves FTP data (HTTP
#       and Gopher protocol support are built into the cache).
#
#       To disable ftpget and the ability to retrieve FTP objects, set
#       this to "none".  Note that ftpget is automatically disabled for
#       http_accel mode.
#
#ftpget_program /usr/local/squid/bin/ftpget
#  TAG: ftpget_options
#       Options for the 'ftpget' program.  Please run 'ftpget' without
#       any arguments to see a list of options.  The default is
#       no options.  An example is
#
#       ftpget_options -n 60 -R -W
#
#ftpget_options
# If you want the anonymous login password to be more informative
# (and enable the use of picky ftp servers), set this to something
```

```
# resonable for your domain, like wwwuser@somewhere.net
#
# The reason why this is domainless by default is that the
# request can be made on the behalf of a user in any domain,
# depending on how the cache is used.
# Some ftp server also validate that the email address is valid
# (for example perl.com).
#
ftp_user ftpuser_name@
#  TAG: cache_dns_program
#       Specify the location of the executable for dnslookup process.
#
#cache_dns_program /usr/local/squid/bin/dnsserver
#  TAG: dns_children
#       The number of processes spawn to service DNS name lookups.
#       For heavily loaded caches on large servers, you should
#       probably increase this value to at least 10.  The maximum
#       is 32.  The default is 5.
#
#       To disable dnsservers, set this to 0.  NOTE, this is very
#       strongly discouraged.  If you disable dnsservers your Squid
#       process will BLOCK on DNS lookups!
#
#dns_children 5
#  TAG: dns_defnames
#       Normally the 'dnsserver' disables the RES_DEFNAMES resolver
#       option (see res_init(3)).  This prevents caches in a hierarchy
#       from interpreting single-component hostnames locally.  To allow
#       dnsserver to handle single-component names, enable this
#       option.
#
#dns_defnames off
#  TAG: unlinkd_program
#       Specify the location of the executable for file deletion process.
#
#unlinkd_program /usr/local/squid/bin/unlinkd
#  TAG: pinger_program
#       Specify the location of the executable for the pinger process.
#
#pinger_program /usr/local/squid/bin/pinger
#  TAG: redirect_program
#       Specify the location of the executable for the URL redirector.
#       Currently, you must provide your own redirector program.
#       See the Release-Notes for how to write one.
#       By default, the redirector is not used.
#
#redirect_program /bin/false
#  TAG: redirect_children
#       The number of redirector processes to spawn.
#
#redirect_children 5

# OPTIONS FOR TUNING THE CACHE
#-----------------------------------------------------------------------------
--

#  TAG: wais_relay
#       Relay WAIS request to host (1st arg) at port (2 arg).
#
#wais_relay localhost 8000
#  TAG: request_size
#       Maximum allowed request size in kilobytes.  If people are using
#       POST to upload files, then set this to the largest acceptable
#       filesize plus a few extra kbytes.
```

```
#
#request_size 150
#  TAG: refresh_pattern         # case sensitive
#  TAG: refresh_pattern/i       # case insensitive
#
#       usage: refresh_pattern regex min percent max
#
#       min and max are specified in MINUTES.
#       percent is an integer number.
#
#       Please see the file doc/Release-Notes-1.1.txt for a full
#       description of Squid's refresh algorithm.  Basically a
#       cached object is:
#
#               FRESH if age < min
#               STALE if expires < now
#               STALE if age > max
#               FRESH if lm-factor < percent
#
#       The refresh_pattern lines are checked in the order listed here.
#       The first entry which matches is used.  If none of the entries
#       match, then the default will be used.
#
#Default:
refresh_pattern         .       0 20% 4320
#  TAG: reference_age
#       As a part of normal operation, Squid performs Least Recently
#       Used removal of cached objects.  The LRU age for removal is
#       computed dynamically, based on the amount of disk space in
#       use.  The 'reference_age' value defines the maximum LRU age.
#       For example, setting reference_age to '1 week' will cause
#       objects to be removed if they have not been accessed for a week
#       or more.  If set to zero, LRU removal is disabled, and objects
#       will be removed only when disk usage is over the high water
#       mark.  The default value is one year.
#
#       Specify a number here, followed by units of time.  For example:
#               1 week
#               3.5 days
#               4 months
#               2.2 hours
#
reference_age 1 year

#  TAG: quick_abort
#       By default the cache continues to retrieve objects from
#       aborted requests.  This may be undesirable on slow (e.g. SLIP)
#       links and/or very busy caches.  Impatient users may tie up
#       file descriptors by repeatedly aborting and re-requesting
#       non-cachable objects.
#
#       Usage: quick_abort    min-kbytes percent max-kbytes
#
#       When the user aborts a request, Squid will check the
#       quick_abort values to the amount of data transfered until
#       then.
#
#       If the transfer has less than 'min-kbytes' remaining, it
#       will finish the retrieval.  Setting minlength to -1 will
#       disable the quick_abort feature.
#
#       If the transfer has more than 'max-kbytes' remaining, it
#       will abort the retrieval.
#
```

```
#       If more than 'percent' of the transfer has completed, it will
#       finish the retrieval.
#
#quick_abort    min percent max
#  TAG: negative_ttl (minutes)
#       Time-to-Live (TTL) for failed requests.  Certain types of
#       failures (such as "connection refused" and "404 Not Found") are
#       negatively-cached for a small amount of time.  The default is 5
#       minutes.  Note that this is different from negative caching of
#       DNS lookups.
#
#negative_ttl 5

#
#  TAG: positive_dns_ttl (minutes)
#       Time-to-Live (TTL) for positive caching of successful DNS lookups.
#       Default is 6 hours (360 minutes).  If you want to minimize the
#       use of Squid's ipcache, set this to 1, not 0.
#
#positive_dns_ttl 360
#  TAG: negative_dns_ttl (minutes)
#       Time-to-Live (TTL) for negative caching of failed DNS lookups.
#
#negative_dns_ttl 5

# TIMEOUTS
#-----------------------------------------------------------------------------
--

#  TAG: connect_timeout (seconds)
#       Some systems (notably Linux) can not be relied upon to properly
#       time out connect(2) requests.  Therefore the squid process
#       enforces its own timeout on server connections.  This parameter
#       specifies how long to wait for the connect to complete.  The
#       default is two minutes (120 seconds).
#
#connect_timeout 120
#  TAG: read_timeout (minutes)
#       An active connection will be aborted after read_timeout minutes
#       of no activity on that connection (i.e., assume the remote server
#       or network connection died after the connection was established).
#       The default is 15 minutes.
#
#read_timeout 15
#  TAG: client_lifetime (minutes)
#       The maximum amount of time that a client (browser) is allowed to
#       remain connected to the cache process.  This protects the Cache
#       from having alot of sockets (and hence file descriptors) tied up
#       in a CLOSE_WAIT state from remote clients that go away without
#       properly shutting down (either because of a network failure or
#       because of a poor client implementation).  The default is three
#       hours, 20 minutes.
#
#       NOTE:  The default value is designed with low-speed client
#       connections in mind.  200 minutes should be plenty of time to
#       transfer a 10M file at 1k/sec.  If you have high-speed client
#       connectivity, or occasionally run out of file descriptors,
#       we suggest you lower this value appropriately.
#
#client_lifetime 200
#  TAG: shutdown_lifetime (seconds)
#
#       When SIGTERM or SIGHUP is received, the cache is put into
#       "shutdown pending" mode until all active sockets are closed.
```

```
#       This value is the lifetime to set for all open descriptors
#       during shutdown mode.  Any active clients after this many
#       seconds will receive a 'lifetime expire' message
#
#shutdown_lifetime 30
# ACCESS CONTROLS
#-----------------------------------------------------------------------------
--

# Defining an Access List
#
# acl aclname acltype string1 ...
# acl aclname acltype "file" ...
#
# when using "file", the file should contain one item per line
#
# acltype is one of src dst srcdomain dstdomain url_pattern urlpath_pattern
#                   time port proto method browser user
#
# acl aclname src      ip-address/netmask ... (clients IP address)
# acl aclname src      ip-address/netmask ... (clients IP address)
# acl aclname src      addr1-addr2/netmask ... (range of addresses)
# acl aclname dst      ip-address/netmask ... (URL host's IP address)
# acl aclname srcdomain   foo.com ... (taken from reverse DNS lookup)
# acl aclname dstdomain   foo.com ... (taken from the URL)
# acl aclname time     [day-abbrevs]  [h1:m1-h2:m2]
#       day-abbrevs:
#               S - Sunday
#               M - Monday
#               T - Tuesday
#               W - Wednesday
#               H - Thursday
#               F - Friday
#               A - Saturday
#       h1:m1 must be less than h2:m2
# acl aclname url_regex  ^http:// ...   # regex matching on whole URL
# acl aclname urlpath_regex  \.gif$ ... # regex matching on URL path only
# acl aclname port     80 70 21 ...
# acl aclname proto    HTTP FTP ...
# acl aclname method   GET POST ...
# acl aclname browser  regexp
# acl aclname user     username ...     # string match on ident output.
#                                       # use REQUIRED to accept any
#                                       # non-null ident.

acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl all src 0.0.0.0/0.0.0.0
acl inside src 192.168.1.0/255.255.255.0
acl inside src 192.168.1.0/255.255.255.0
acl example src 192.168.1.113/255.255.255.255
acl SSL_ports port 443 563
acl Dangerous_ports port 7 9 19
acl CONNECT method CONNECT

# Allowing or Denying access based on defined access lists
#
# Access to the HTTP port:
#     http_access allow|deny [!]aclname ...
#
# Access to the ICP port:
#     icp_access  allow|deny [!]aclname ...
#
# NOTE on default values:
```

```
#
#       If there are no “access” lines present, the default is to allow
#       the request.
#
#       If none of the “access” lines cause a match, the default is the
#       opposite of the last line in the list.  If the last line was
#       deny, then the default is allow.  Conversely, if the last line
#       is allow, the default will be deny.  For these reasons, it is a
#       good idea to have an “deny all” or “allow all” entry at the end
#       of your access lists to avoid potential confusion.


# Only allow access to the cache manager functions from the local host.
#http_access deny manager !localhost
http_access allow manager localhost
http_access deny manager
http_access deny CONNECT !SSL_ports
http_access deny CONNECT !SSL_ports
http_access deny CONNECT !SSL_ports
http_access deny Dangerous_ports
#http_access allow localclients
http_access allow manager example
# Allow everything else
http_access allow inside
http_access allow localhost
http_access allow all
#http_access allow localclients

# Reply to all ICP queries we receive
icp_access  deny  all
#icp_access  allow localclients

#  TAG: miss_access
#       Use to force your neighbors to use you as a sibling instead of
#       a parent.  For example:
#
#               acl localclients src 172.16.0.0/16
#               miss_access allow localclients
#               miss_access deny  !localclients
#
#       This means that only your local clients are allowed to fetch
#       MISSES and all other clients can only fetch HITS.
#
#       By default, allow all clients who passed the http_access rules
#       to fetch MISSES from us.
#
miss_access allow  all
miss_access allow manager
#  TAG: cache_host_acl
#       Just like ‘cache_host_domain’ but provides more flexibility by
#       using ACL’s.
#
#               cache_host_acl cache-host       [!]aclname ...
#
#       NOTE:   * Any number of ACL’s may be given for a cache-host,
#                 either on the same or separate lines.
#               * When multiple ACL’s are given for a particular
#                 cache-host, the first matched ACL is applied.
#               * Cache hosts with no domain or ACL restrictions are
#                 queried for all requests.
#               * There are no defaults.


# ADMINISTRATIVE PARAMETERS
```

```
#-----------------------------------------------------------------------------
--

#  TAG: cache_mgr
#       Email-address of local cache manager who will receive
#       mail if the cache dies.  The default is "webmaster."
#
cache_mgr iclab-admin
#  TAG: cache_effective_user
#       If the cache is run as root, it will change its effective/real
#       UID/GID to the UID/GID specified below.  The default is not to
#       change UID/GID.
#
#cache_effective_user nobody nogroup
cache_effective_user andree staff


#  TAG: visible_hostname
#       If you want to present a special hostname in error messages, etc,
#       then define this.  Otherwise, the return value of gethostname()
#       will be used.
#
#visible_hostname www-cache.foo.org

# OPTIONS FOR THE CACHE REGISTRATION SERVICE
#-----------------------------------------------------------------------------
--

#       This section contains parameters for the (optional) cache
#       announcement service.  This service is provided to help
#       cache administrators locate one another in order to join or
#       create cache hierarchies.
#
#       An 'announcement' message is sent (via UDP) to the registration
#       service by Squid.  By default, the annoucement message is NOT
#       SENT unless you enable it with 'cache_announce' below.
#
#       The announcement message includes your hostname, plus the
#       following information from this configuration file:
#
#               http_port
#               icp_port
#               cache_mgr
#
#       All current information is processed regularly and made
#       available on the Web at http://www.nlanr.net/Cache/Tracker/.


# This is how frequently to send cache announcements.  The default
# is '0' which disables sending the announcement messages.
#
# To enable announcing your cache, just uncomment the line below.
#
#cache_announce 24
# This is the hostname and portnumber where the registration message
# will be sent.
#
# Format:       announce_to   host[:port] [filename]
#
# Hostname will default to 'tracker.ircache.net' and port will default
# to 3131.  If the 'filename' argument is given, the contents of that
# file will be included in the announce message.
#
#announce_to tracker.ircache.net:3131
```

```
# HTTPD-ACCELERATOR OPTIONS
#-----------------------------------------------------------------------------
--

#  TAG: httpd_accel
#       If you want to run squid as an httpd accelerator, define the
#       host name and port number where the real HTTP server is.
#
#       If you want virtual host support then specify the hostname
#       as “virtual”.
#
#httpd_accel real_httpd_host real_httpd_port
#  TAG: httpd_accel_with_proxy
#       If you want to use squid as both a local httpd accelerator
#       and as a proxy, change this to ‘on’.
#
#httpd_accel_with_proxy off
#  TAG: httpd_accel_uses_host_header
#       HTTP/1.1 requests include a Host: header which is basically the
#       hostname from the URL.  Squid can be an accelerator for
#       different HTTP servers by looking at this header.  However,
#       Squid does NOT check the value of the Host header, so it opens
#       a big security hole.  We recommend that this option remain
#       disabled unless you are sure of what you are doing.
#
#httpd_accel_uses_host_header off

# MISCELLANEOUS
#-----------------------------------------------------------------------------
--

# The DNS tests exit as soon as the first site is successfully looked up
#
# If you want to disable DNS tests, do not comment out or delete this
# list.  Instead use the -D command line option
#
dns_testnames internic.net usc.edu cs.colorado.edu mit.edu yale.edu
#  TAG: logfile_rotate #
#       Specifies the number of logfile rotations to make upon receiving
#       a USR1 signal.  The default is 10, which will rotate with
#       extensions 0 through 9.  Setting logfile_rotate to 0 will
#       disable the rotation, but the logfiles are still closed and
#       re-opened.  This will enable you to rename the logfiles yourself
#       just before sending a USR1 signal to the squid process.
#
logfile_rotate 10
#  TAG: append_domain
#       Appends local domain name to hostnames without any dots in them.
#       append_domain must begin with a period.
#
#append_domain .ce.nihon-u.ac.jp
#  TAG: tcp_recv_bufsize
#       Size of receive buffer to set for TCP sockets.  Probably just
#       as easy to change your kernel’s default.  Set to zero to use
#       the default buffer size.
#
#tcp_recv_bufsize 0

#  TAG: ssl_proxy
#       Specify the name of a ‘cache_host’ listed above, or a hostname
#       and port number where all SSL requests should be forwarded to.
#
#       Usage: ssl_proxy cache_host
```



```
#               ssl_proxy host:port
#
#ssl_proxy
#  TAG: passthrough_proxy
#       Specify the name of a 'cache_host' listed above, or a hostname
#       and port number where all non-GET (i.e. POST, PUT) requests
#       should be forwarded to.
#
#       Usage: passthrough_proxy cache_host
#              passthrough_proxy host:port
#
#passthrough_proxy
#  TAG: proxy_auth
#       Usage: proxy_auth passwd_file [ ignore-domain ]
#
#       'passwd_file' is an apache-style file of passwords for
#       authenticated proxy access Looks like user:password, with the
#       password being standard crypt() format.  Proxy authentication
#       is disabled by default.
#
#       'ignore-domain' is a domain name for which authorization will
#       not be required.
#
#       NOTE, proxy_auth support is not compiled into Squid by default.
#       To use this feature you must enable the USE_PROXY_AUTH option
#       near the top of src/Makefile.
#
#proxy_auth /dev/null
#  TAG: err_html_text
#       HTML text to include in error messages.  Make this a "mailto"
#       URL to your admin address, or maybe just a link to your
#       organizations Web page.
#
#err_html_text
#  TAG: deny_info
#       Usage: deny_info URL acl
#
#       This can be used to return a HTTP redirect for requests which
#       do not pass the 'http_access' rules.  A single ACL will cause
#       the http_access check to fail.  If a 'deny_info' line exists
#       for that ACL then Squid returns a redirect to the given URL.

#  TAG: udp_hit_obj on|off
#       If set, Squid will request UDP_HIT_OBJ replies from its
#       neighbors.  UDP_HIT_OBJ is nice because it saves bandwidth, but
#       it can cause some other problems.  For one it complicates
#       calculating hit rates.  Also, problems arise because the ICP
#       query does not contain any HTTP request headers which may
#       affect the reply.
#
#udp_hit_obj off
#  TAG: udp_hit_obj_size
#
#     If set, Squid will limit UDP_HIT_OBJ size to be less than
#     this value.  Setting this value to more than SQUID_UDP_SO_SNDBUF
#     will not work as expected.  Set to zero to select the size
#     permited by the socket.
#udp_hit_obj_size     0

#  TAG: memory_pools on|off
#       If set, Squid will keep pools of allocated (but unused) memory
#       available for future use.  If memory is a premium on your
#       system, disable this.
#
```

```
#memory_pools on
#  TAG: forwarded_for on|off
#       If set, Squid will include your system's IP address or name
#       in the HTTP requests it forwards.  By default it looks like
#       this:
#
#               X-Forwarded-For: 192.1.2.3
#
#       If you disable this, it will appear as
#
#               X-Forwarded-For: unknown
#
#forwarded_for on
#  TAG: log_icp_queries on|off
#       If set, ICP queries are logged to access.log.  ICP logging
#       is enabled by default, so uncomment and change the line
#       below to disable it.
#
#log_icp_queries on

#  TAG: minimum_direct_hops
#       If using the ICMP pinging stuff, do direct fetches for sites
#       which are no more than this many hops away.
#
minimum_direct_hops 4
#  TAG: cachemgr_passwd
#       Specify passwords for cachemgr operations.
#
#Usage: cachemgr_passwd password action action ...
#
#       valid actions are:
#               shutdown *
#               info
#               stats/objects
#               stats/vm_objects
#               stats/utilization
#               stats/ipcache
#               stats/fqdncache
#               stats/dns
#               stats/redirector
#               stats/io
#               stats/reply_headers
#               stats/filedescriptors
#               stats/netdb
#               log/status *
#               log/enable *
#               log/disable *
#               log/clear *
#               log *
#               parameter
#               server_list
#               client_list
#               squid.conf *
#
#       * Indicates actions which will not be performed without a
#         valid password, others can be performed if not listed here.
#
#       To disable an action, set the password to "disable".
#       To allow performing an action without a password, set the
#       password to "none".
#
#       Use the keyword "all" to set the same password for all actions.
#
#Examples:
```

```
#
#       cachemgr_passwd secret shutdown
#       cachemgr_passwd lessssssecret info stats/objects
#       cachemgr_passwd disable all
#
#Defaults: none
#  TAG: swap_level1_dirs
#       Number of first-level directories to create for storing cached
#       objects.  Minimum 1, maximum 256, default 16.
#
#swap_level1_dirs 16
#  TAG: swap_level2_dirs
#       Number of sub-directories to create under each first-level
#       directory.  Minimum 1, maximum 256, default 256.
#
#swap_level2_dirs 256
#  TAG: store_avg_object_size
#       Average object size, used to estimate number of objects your
#       cache can hold.  See doc/Release-Notes-1.1.txt.  The default is
#       13K.
#
#store_avg_object_size 13
#  TAG: store_objects_per_bucket
#       Target number of objects per bucket in the store hash table.
#       Lowering this value increases the total number of buckets and
#       also the storage maintenance rate.  The default is 20.
#
#store_objects_per_bucket 20
#  TAG: http_anonymizer
#       If you want to filter out certain HTTP request headers for
#       privacy reasons, enable this option.  There are three
#       appropriate settings:
#               'off'           All HTTP request headers are passed.
#               'standard'      Specific headers are removed
#               'paranoid'      Only specific headers are allowed.
#       To see which headers are allowed or denied, please see the
#       http-anon.c source file.
#
#http_anonymizer off
#  TAG: fake_user_agent
#       If you use the paranoid http_anonymizer setting, Squid will strip
#       your User-agent string from the request.  Some Web servers will
#       refuse your request without a User-agent string.  Use this to
#       fake one up.  For example:
#
#       fake_user_agent Nutscrape/1.0 (CP/M; 8-bit)
#       (credit to Paul Southworth pauls@etext.org for this one!)
#
#fake_user_agent none
#  TAG: client_db
#       If you want to disable collecting per-client statistics, then
#       turn off client_db here.
#
#client_db on
#  TAG: netdb_low
#  TAG: netdb_high
#       The low and high water marks for the ICMP measurement
#       database.  These are counts, not percents.  The defaults are
#       900 and 1000.  When the high water mark is reached, database
#       entries will be deleted until the low mark is reached.
#
#netdb_low 900
#netdb_high 1000
```

```
#  TAG: netdb_ping_rate
#       The minimum period for measuring a site.  There will be at
#       least this much delay between successive pings to the same
#       network.  The default is five minutes.
#
#netdb_ping_period 5 minutes
#  TAG: query_icmp
#       If you want to ask your peers to include ICMP data in their ICP
#       replies, enable this option.
#
#       If your peer has built squid with '-DUSE_ICMP=1' then that peer
#       will send ICMP pings to origin server sites of the URLs it
#       receives.  If you enable this option then the ICP replies from
#       that peer will include the ICMP data (if available).  Then,
#       when choosing a parent cache, Squid will choose the parent with
#       the minimal RTT to the origin server.  When this happens, the
#       hierarchy field of the access.log will be
#       "CLOSEST_PARENT_MISS".  This option is off by default.
#
#query_icmp off
#  TAG: icp_hit_stale
#       If you want to return ICP_HIT for stale cache objects, set this
#       option to 'on'.  If you have sibling relationships with caches
#       in other administrative domains, this should be 'off'.  If you only
#       have sibling relationships with caches under your control, then
#       it is probably okay to set this to 'on'.  NEVER enable
#       icp_hit_stale if you also use 'miss_access'.
#
#icp_hit_stale off
#  TAG: minimum_retry_timeout (Mike Pelletier )
#       This specifies the minimum connect timeout for the retry
#       patch, for instances when the connect timeout is reduced
#       to compensate for the availability of multiple IP addresses.
#
#       When a connection to a host is initiated, and that host has
#       several IP addresses, the default connection timeout is
#       reduced by dividing it by the number of addresses.  So,
#       a site with 15 addresses would then have a timeout of 8
#       seconds for each address attempted.  To avoid having the
#       timeout reduced to the point where even a working host
#       would not have a chance to respond, this setting is
#       provided. The default, and the minimum value, is five
#       seconds, and the maximum value is sixty seconds, or half of
#       connect_timeout, whichever is greater and less than
#       connect_timeout.  This feature is not compiled in by
#       default.  You must add -DRETRY_PATCH in src/Makefile.
#
#minimum_retry_timeout 5
#  TAG: maximum_single_addr_tries
#       This sets the maximum number of connection attempts for a
#       host that only has one address (for multiple-address hosts,
#       each address is tried once) for the retry patch.
#
#       The default value is three tries, the (not recommended)
#       maximum is 255 tries.  A warning message will be generated if
#       it is set to a value greater than ten.  You must add
#       -DRETRY_PATCH in src/Makefile.
#
#maximum_single_addr_tries 3
#  TAG: reload_into_ims
#       Enable this if you want to turn 'Pragma: no-cache' requests
#       into If-Modified-Since requests.  Off by default, use at your
#       own risk.  This feature is not compiled in by default.  You
#       must add -DRELOAD_INTO_IMS in src/Makefile.
```

```
#
#reload_into_ims off
#Original design: Andree Toonk! 26-04-2000
```

Figuur 227: Voorbeeldconfiguratie Squid 2.2 stable 5

30. Bijlage C: FrontPage® web

Dit is een beknopte handleiding van de werking van de FrontPage Client en hoe u hiermee uw website kunt onderhouden. In deze bijlage worden de volgende onderwerpen behandeld:

- Wat is FrontPage?
- Beginnen met FrontPage.
- Maken van een website.
- De eerste pagina.
- Beheren van de website.

In de daaropvolgende paragrafen wordt dieper ingegaan op de volgende onderwerpen.

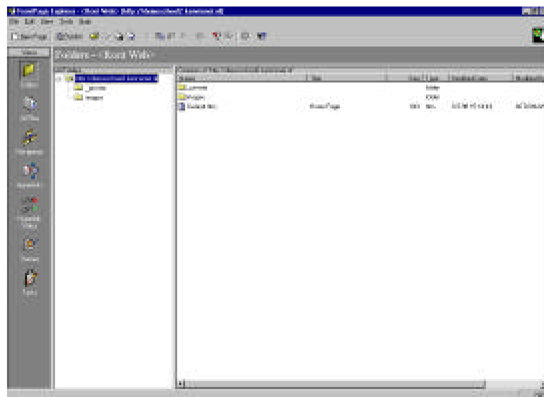
- FrontPage Explorer
- FrontPage Editor

30.1 Wat is FrontPage?

FrontPage is een programma om op een eenvoudige manier websites te maken en te beheren. FrontPage biedt hiervoor verschillende onderdelen.

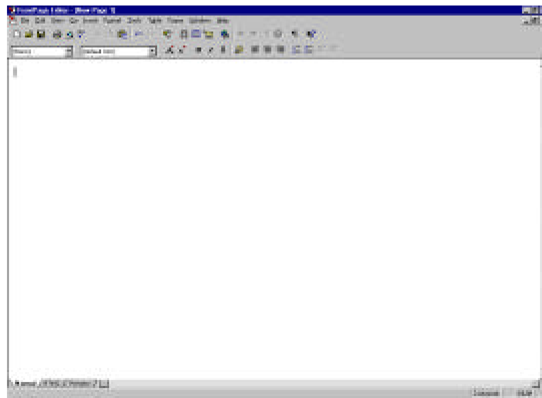
- FrontPage Explorer
- FrontPage Editor
- Microsoft Image Composer

U kunt uw website eenvoudig bekijken, beheren en besturen met behulp van de grafische tools van de ingebouwde FrontPage Explorer. FrontPage Explorer biedt u bijvoorbeeld een duidelijk inzicht in de structuur van uw website en van de daarin opgenomen hyperlinks (zie Figuur 228). Meer functies van FrontPage Explorer vindt u in paragraaf 30.4.



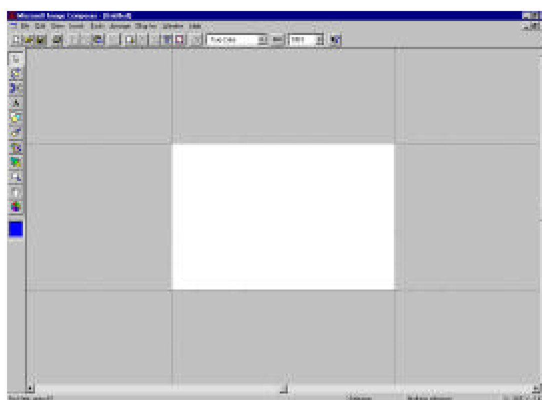
Figuur 228: FrontPage Explorer

Het aanbrengen van hyperlinks en het toevoegen van informatie uit applicaties of gegevensbestanden gaat als vanzelf met de zeer visuele FrontPage Editor (zie Figuur 229).Voor een uitgebreide beschrijving kunt u terecht in paragraaf 30.3.



Figuur 229: FrontPage Editor

Met Microsoft Image Composer kunt u zelf illustraties maken voor uw website of er foto's in opnemen (zie Figuur 230). Dit programma staat op de FrontPage CD-ROM en kan samen met de FrontPage Client worden geïnstalleerd.

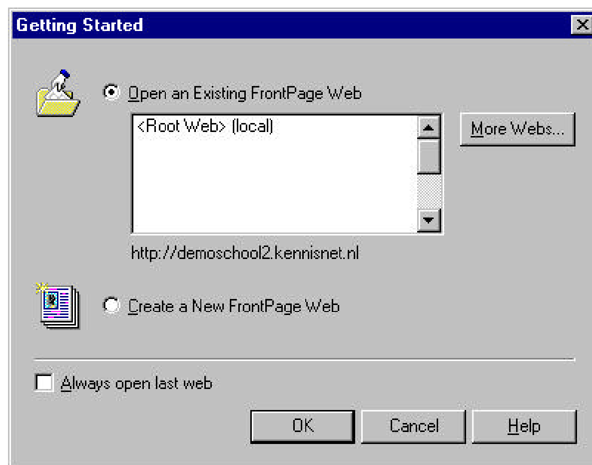


Figuur 230: Microsoft Image Composer

30.2 Beginnen met FrontPage

Er wordt hier vanuit gegaan dat de FrontPage Client reeds is geïnstalleerd. Er is alleen een Engelse versie beschikbaar. Om een nieuwe website op te bouwen, gaat u als volgt te werk.

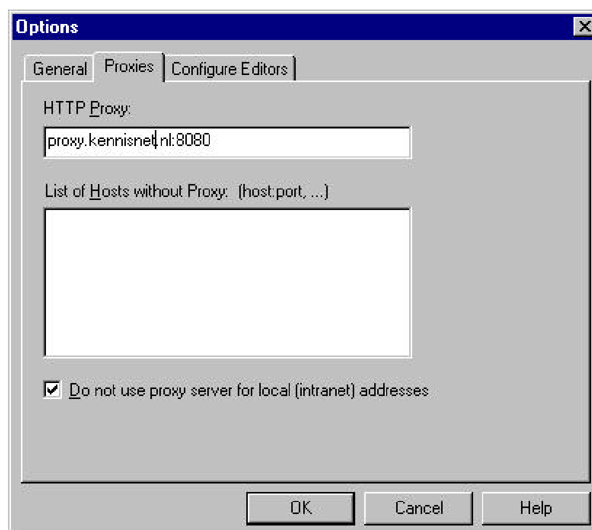
Start de FrontPage Client via het 'Start'-menu van Windows. Het volgende scherm, zoals weergegeven in Figuur 231, verschijnt.



Figuur 231: FrontPage: Startvenster ('Getting Started')

U kunt hier aangeven of u met een bestaande website of een nieuwe website aan de slag wilt.

Indien u dit nog niet heeft ingesteld en vanuit kennisnet uw website bijwerkt, dient u echter eerst de instellingen voor de webproxy in te vullen. Klik dan eerst op 'Cancel'. Het scherm van de FrontPage Explorer verschijnt. Selecteer uit het menu 'Tools' de keuze 'Options…'. Er verschijnt een venster, zoals in Figuur 232.



Figuur 232: Options, Proxies

Ga naar het tabblad 'Proxies'. In het veld 'HTTP Proxy:' dient u het adres van de proxies van kennisnet in te vullen, gevolgd door een dubbele punt en het poortnummer: `proxy.kennisnet.nl:8080`.

Klik op 'OK' om de instellingen te activeren.

U bevindt zich weer in de FrontPage Explorer. Selecteer uit het menu 'File' de keuze 'Open FrontPage Web'. Er verschijnt weer een venster zoals in Figuur 231.

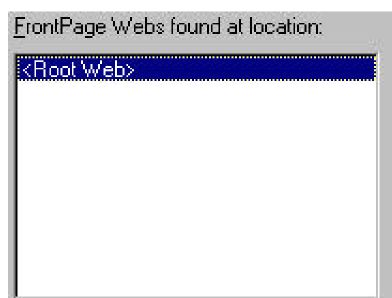
Klik op de knop 'More Webs…'. Vervolgens verschijnt het venster zoals getoond in Figuur 233.



Figuur 233: Open FrontPage Web

Vul bij: ‘Select a Web server or disk location’ de naam in van de website (het internetadres) zoals u die van kennisnet heeft gekregen. Dit is, volgens de geldende standaard, een naam in de vorm van: ‘`<schoolnaam>.<plaatsnaam>.kennisnet.nl`’.

Klik vervolgens op de knop: ‘List webs’. In het venster: ‘FrontPage Webs found at location:’ verschijnt een lijst van de websites.



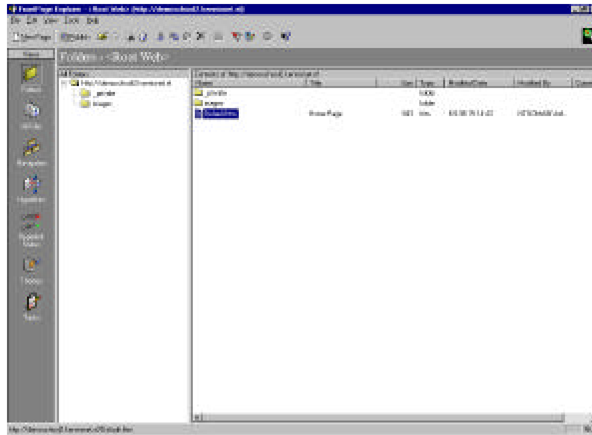
Figuur 234: FrontPage: Lijst met locaties

Dubbelklik op <Root Web>.
In het scherm dat nu verschijnt, kunt u een loginnaam en wachtwoord invoeren (Figuur 235).



Figuur 235: Name and Password Required

Vul hier de gebruikersnaam en het wachtwoord in die u hebt gekregen van kennisnet.
Het FrontPage Explorer-scherm verschijnt, waarmee u kunt navigeren binnen uw website.



Figuur 236: FrontPage Explorer

30.3 De eerste pagina

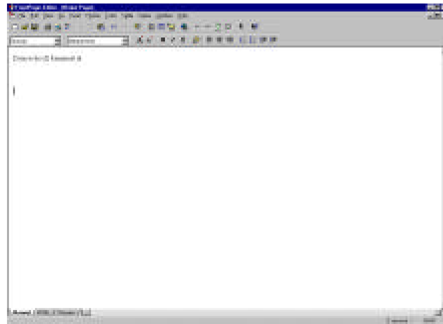
Zodra u uw website hebt geopend, is het mogelijk om pagina's aan te maken of te bewerken. Het scherm van de FrontPage Explorer lijkt op dat van de verkenner van Windows 95/98 of Windows NT-verkenner.

Rechts bevindt zich het scherm waarin u de bestanden kunt zien ('Contents' of '`http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/`'). Aan de linkerkant ziet u een boomstructuur zoals u die ook kent van de verkenner (All folders). Hier kunt u bladeren door de mappen die zich op uw webserver bevinden. In het venster aan de rechterkant kunt u vervolgens op de pagina's dubbelklikken om die te bewerken.

Ook is het mogelijk om een nieuwe pagina aan te maken. Hiervoor klikt u met de rechtermuisknop in het rechter scherm. Selecteer vervolgens: 'New page'. Er wordt een nieuwe pagina aangemaakt die u vervolgens een naam kunt geven. Als u vervolgens op de naam dubbelklikt, wordt de FrontPage Editor geopend waarmee de pagina kan worden bewerkt.

Standaard staat er een pagina op de webserver die '`default.htm`' heet. Dit is de pagina die de server zal tonen zodra men het adres van uw website in een bladerprogramma (internet-browser) intypt:
`http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/`
Deze pagina kunt u naar eigen inzicht aanpassen door erop te dubbelklikken. De FrontPage Editor wordt geopend en de pagina kan worden bewerkt.

Als het de eerste keer is dat de pagina wordt bewerkt, wordt er door kennisnet een pagina aangemaakt waarop de naam van de website staat vermeld (Figuur 237).



Figuur 237: FrontPage Standaardpagina

De FrontPage Editor is te vergelijken met het tekstverwerkingsprogramma Microsoft Word. Teksten, tabellen en plaatjes kunnen eenvoudig worden ingevoegd zonder dat er kennis van HTML is vereist. Langs de bovenkant van het scherm bevinden zich enkele werkbalken waar de meest gebruikte functies staan. Voor een uitgebreide beschrijving van de Editor kunt u terecht in de helpfunctie van de FrontPage Editor.

Zodra u de pagina naar uw wensen hebt aangepast, kunt u de pagina opslaan door in de werkbalk op de 'Save'- icoon te klikken. Vanaf dat moment staat de zojuist aangepaste pagina op het internet.

30.4 FrontPage Explorer

Deze subparagraaf is een korte introductie van de FrontPage Explorer. Deze Explorer kan worden vergeleken met de verkenner die wordt geleverd met Windows 95/98 of NT. Het is een grafische representatie van de structuur van de website. Er kan worden gebladerd door de websites, pagina's en mappen kunnen worden aangemaakt. Websites, pagina's en mappen kunnen ook worden gewijzigd of worden verwijderd.

Voor een uitgebreide handleiding kunt u de (Engelstalige) helpfunctie van FrontPage raadplegen.

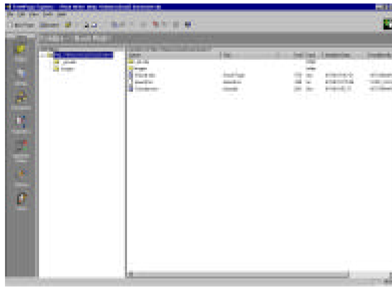
Er is een aantal manieren om de FrontPage Explorer te gebruiken. Binnen het programma worden dat 'views' genoemd. Er zijn verschillende 'views' mogelijk.

- Folders
- All files
- Navigation
- Hyperlinks
- Hyperlink status
- Themes
- Tasks

Hierna worden de verschillende views besproken.

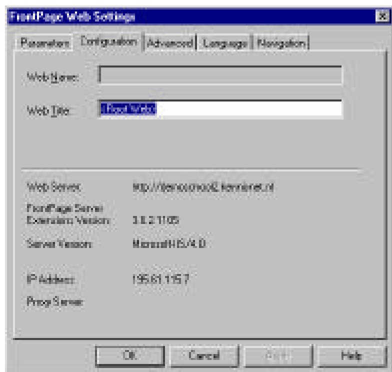
30.4.1 Folders

Dit is de view die automatisch verschijnt, zodra u zich succesvol hebt aangemeld op de webserver (Figuur 238). De meeste handelingen zullen vanuit deze view worden gedaan. De view is te vergelijken met de verkenner die standaard zit bij Windows 95/98 of NT. Met aan de linkerkant de boomstructuur van de website en rechts een venster met de inhoud van de website. Pagina's en mappen kunnen aangemaakt, gewijzigd of verwijderd worden. Dit kan door met de rechter muisknop te klikken in het rechter venster. Er verschijnt een menu waar gekozen kan worden uit: 'New Page' (nieuwe pagina) of 'New Folder' (nieuwe map).



Figuur 238: FrontPage Explorer: View ‘Folders’

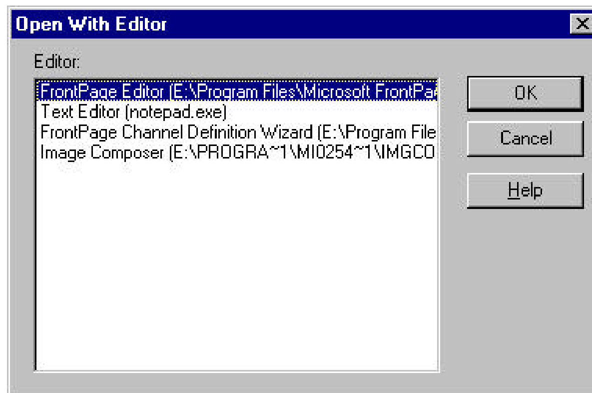
Verder is er nog een optie die ‘Web Settings’ heet (Figuur 239). Hier kunnen enkele algemene instellingen voor de website worden veranderd, waaronder de titel van de website.



Figuur 239: FrontPage Web Settings, Configuration

Als u een document selecteert en vervolgens met de rechter muisknop klikt, krijgt u een ander menu te zien. Hier kan worden gekozen uit de volgende opties:

- **Open**: het document wordt geopend binnen de FrontPage Editor.
- **Open With Editor**: er verschijnt een scherm waar gekozen kan worden met welk programma het document moet worden geopend (zie Figuur 240). Selecteer het programma waarmee de pagina moet worden geopend en klik op ‘OK’.
- **Cut**: de standaardfunctie knippen.
- **Copy**: de standaardfunctie kopiëren.
- **Rename**: het document een nieuwe naam geven.
- **Delete**: het geselecteerde document verwijderen van de website.
- **Add Task**: hier kan worden aangegeven wat er nog aan de geselecteerde pagina gedaan moet worden.
- **Properties**: u kunt hiermee de eigenschappen van de geselecteerde pagina aanpassen. U kunt hier ook een beschrijving geven van de functie van de pagina of een korte samenvatting van de inhoud. Dit kan dan worden teruggevonden binnen de FrontPage Explorer.

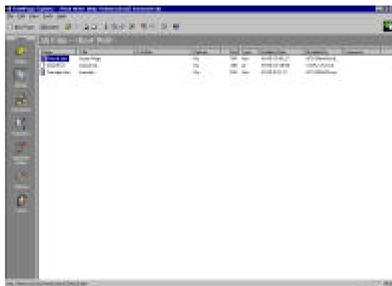


Figuur 240: FrontPage Explorer: Openen met een extern programma

30.4.2 All files

Deze view laat alle bestanden zien die op de website staan, ongeacht de map waar de bestanden staan (Figuur 241).

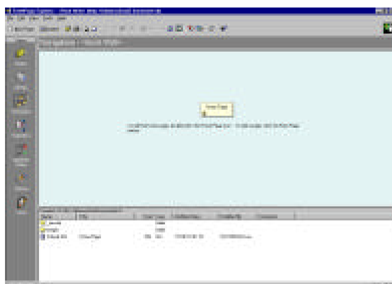
Door in dit scherm met de rechter muisknop te klikken, kan een nieuwe pagina worden aangemaakt. Ook kan hier de naam van een pagina worden veranderd of kan een pagina of plaatje worden verwijderd, zoals hierboven beschreven. In deze view kunnen geen mappen worden aangemaakt of verwijderd.



Figuur 241: FrontPage Explorer: View ‘All files’

30.4.3 Navigation

In deze view is het mogelijk om de navigatie van de website aan te geven (Figuur 242).



Figuur 242: FrontPage Explorer: View ‘Navigation’

FrontPage kan automatisch knoppen of hyperlinks genereren naar andere pagina’s. Door in dit scherm bestanden te slepen naar het hoofddocument, worden automatisch knoppen en links toegevoegd aan de pagina, die ervoor zorgen dat bezoekers van de website de weg kunnen vinden binnen de website.

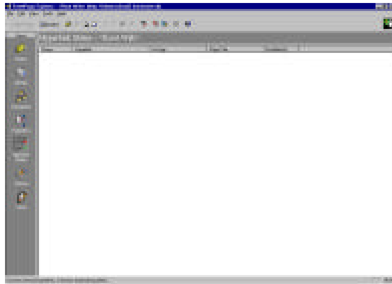
De view bestaat uit twee schermen: het bovenste scherm is een grafische presentatie van de navigatiestructuur. Vanuit het onderste scherm kunnen pagina's die naar elkaar moeten verwijzen, naar de pagina in het bovenste scherm worden 'gesleept'. Dit kan men doen door in het onderste scherm een pagina te selecteren en vervolgens naar het bovenste scherm te slepen waarbij de linker muisknop ingedrukt wordt gehouden.

Op het moment dat het gesleepte document in de buurt komt van een ander document, verschijnt er een lijn van het ene naar het andere document. Op het moment dat de lijn naar de juiste pagina verwijst, moet de linker muisknop worden losgelaten. In de pagina waar de bewuste pagina naartoe is gesleept, komt automatisch een knop die verwijst naar de gesleepte pagina. Zo wordt er door FrontPage automatisch een navigatieboom aangemaakt met hyperlinks of knoppen.

In het onderste scherm kunt u door de website bladeren, zoals ook via de 'Folders' view.

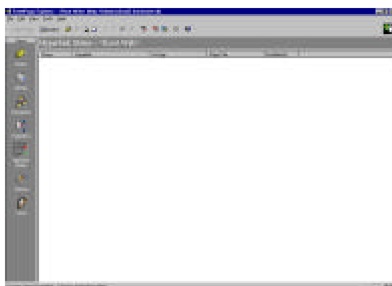
30.4.4 Hyperlinks

In dit scherm kan worden bekeken welke bestanden een link hebben naar de andere pagina's. Op deze manier kan worden bekeken welke invloed bijvoorbeeld het verwijderen van een pagina kan hebben op de andere pagina's.



Figuur 243: FrontPage Explorer: View 'Hyperlinks'

30.4.5 Hyperlink status



Figuur 244: FrontPage Explorer: View 'Hyperlink status'

In de view 'Hyperlink status' wordt bekeken of alle hyperlinks die op de diverse pagina's staan, nog correct zijn. Hierbij wordt gekeken naar zowel links binnen de website als naar links die naar websites gaan die buiten `http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/` liggen.

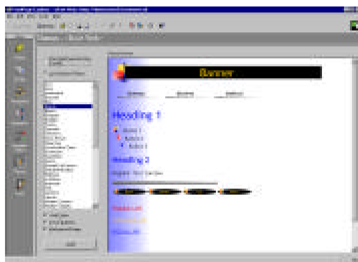
30.4.6 Themes

FrontPage biedt de mogelijkheid om de hele website in een bepaalde opmaak te krijgen. FrontPage heeft hiervoor 'Themes' beschikbaar. Deze thema's kunnen het beste worden vergeleken met de sjablonen zoals die binnen Microsoft Word worden gebruikt. De thema's bevatten informatie over de opmaak van de gehele website, bijvoorbeeld:

- achtergronden;
- lettertype;
- knoppen;
- animaties;
- kleuren van de tekst.

Op het moment dat een bepaald thema is geselecteerd, heeft de website in één keer een totaal andere opmaak. Door een ander thema te selecteren, kan de website er heel anders uitzien. Standaard worden er door Microsoft enkele thema's meegeleverd. Hieruit kan een keus worden gemaakt.

Links kan men uit een lijst een thema selecteren. Rechts ziet men vervolgens een voorbeeld hoe de website eruit kan komen te zien (Figuur 245). Op het moment dat er op 'Apply' wordt geklikt, wordt de website volgens het zojuist gekozen thema opgemaakt.

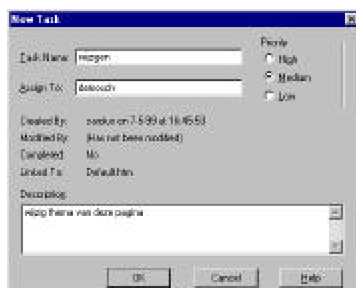


Figuur 245: FrontPage Explorer: View 'Themes'

30.4.7 Tasks

In de view 'Tasks' vindt u een overzicht van taken die nog moeten gebeuren. In alle views is het mogelijk om aan een pagina een taak te verbinden. Deze worden overzichtelijk gegroepeerd onder deze view.

Wanneer u met de rechter muisknop op een bestand klikt in één van de andere views, kan men een taak aanmaken.



Figuur 246: FrontPage Explorer, New Task

Hier kan worden aangegeven:

- de naam van de taak;
- de prioriteit;
- de taak kan eventueel worden voorzien van enig commentaar.

Als er vervolgens op 'OK' wordt geklikt, wordt de taak toegevoegd aan de view 'Tasks'

Binnen de view ‘Task’ kan men met de rechter muisknop klikken op de taak. Men heeft vervolgens de keuze uit de volgende opties:

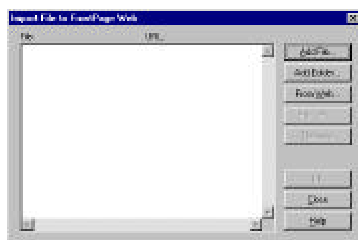
- **Edit Task**: als u hierop klikt, kunt u de gegevens van de taak wijzigen. Hetzelfde scherm als in Figuur 246 verschijnt.
- **Do Task**: bij het selecteren van deze optie wordt de FrontPage Editor opgestart, waarna de pagina waarbij de taak hoorde, kan worden bewerkt.
- **Mark Complete**: ongeacht of de taak is gedaan of niet, kan hier worden aangegeven dat de taak ‘af’ is.
- **Delete**: met deze keuze verwijdert u de taak.

Dit zijn de basisbeginselen van de FrontPage Explorer. Voor een uitgebreider handleiding wordt verwezen naar de helpfunctie die overal aanwezig is binnen de FrontPage Explorer.

30.5 Oude website importeren

Wanneer u reeds een andere (‘oude’) website hebt, kan deze geïmporteerd worden op de nieuwe kennisnet-website. Hiervoor moeten de volgende handelingen worden verricht.

Open in FrontPage uw webserver bij kennisnet, zoals dat eerder in dit document staat beschreven. Klik op ‘File’ in het menu en klik vervolgens op ‘Import…’. Er verschijnt een scherm zoals in Figuur 247.

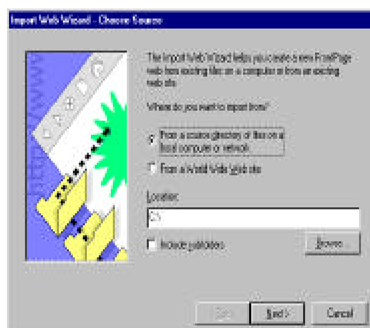


Figuur 247: Import File to FrontPage Web

Binnen dit scherm zijn er drie mogelijkheden.

- **Add File**: er kan een bestand worden ingevoegd.
- **Add Folder**: er kan een map worden ingevoegd.
- **From Web**: een bestaande website kan worden geïmporteerd op de kennisnet-webserver.

In dit voorbeeld wordt er vanuit gegaan dat er een bestaande website is die wordt geïmporteerd. Als er op de knop: ‘From Web...’ wordt geklikt, verschijnt het volgende scherm.

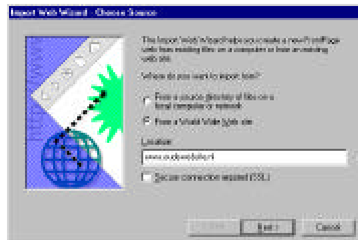


Figuur 248: Import Web Wizard - Choose Source

Er kan worden aangegeven of de pagina’s zich op het lokale netwerk bevinden, of dat men al ergens een website heeft. Indien er al ergens een website bij een provider staat, kan op: ‘From a World Wide Web site’ worden geklikt.

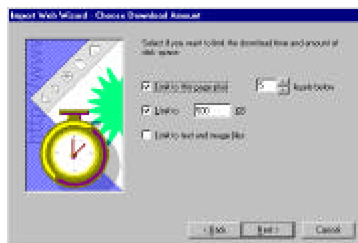
Staat de website ergens op het netwerk of de lokale harde schijf, dan kan er op: ‘From a source directory or files on a local computer or network’ worden geklikt.

In het volgende voorbeeld wordt er vanuit gegaan dat de website al ergens op internet staat en dat er gekozen is voor de optie: ‘From a World Wide Web site’. Het volgende scherm verschijnt (Figuur 249).



Figuur 249: Import Web Wizard - Choose Source: oude website

Hier kan de oude website worden geselecteerd en kan er worden aangegeven of de onderliggende mappenstructuur van de website wordt meegenomen. Dit doet men door op het aankruisvak ‘Include subfolders’ te klikken. Voer de naam van de te importeren website in bij ‘Location’. Klik op ‘Next>’ om naar het volgende scherm te gaan.



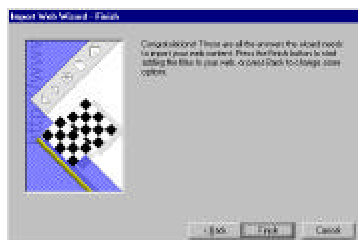
Figuur 250: Import Web Wizard - Choose Download Amount

Binnen dit scherm kan worden opgegeven hoe ‘diep’ de oude website geïmporteerd moet worden. Dat wil zeggen: hoeveel niveaus van de bestandsstructuur (in hyperlinks) geïmporteerd dienen te worden. Waarschijnlijk zult u hier geen limiet aan willen stellen, wanneer u de *gehele* website wilt overnemen.

Ook kan worden opgegeven hoe groot (in kilobytes) in totaal de bestanden mogen zijn, die geïmporteerd gaan worden. Hier zult u eveneens geen limiet willen stellen wanneer u de *gehele* website wilt overnemen.

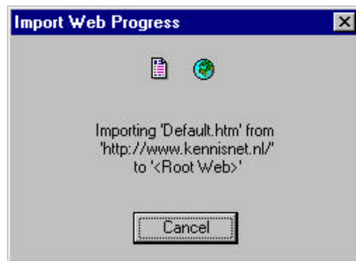
Tot slot kunt u aangeven dat alleen teksten en afbeeldingen (en niet bijvoorbeeld Java-applets, filmpjes en geluiden) geïmporteerd mogen worden.

Klik op ‘Next>’ om op het laatste scherm van de Import Web Wizard terecht te komen (Figuur 251).



Figuur 251: Import Web Wizard - Choose Source, Finish

Klik op ‘Finish’ om de website te importeren. Hier kan enige tijd overheen gaan. Vooral als er veel plaatjes staan op de oude website, kan het enige tijd duren. In de tussentijd ziet u het volgende scherm.



Figuur 252: Import Web Progress: Importstatus

Pagina’s met dezelfde namen worden overschreven. Zodra de website is geïmporteerd, kan deze bewerkt worden op de gebruikelijk FrontPage-manier.

31. Bijlage D: Indeling IP-adresreeksen

Deze bijlage gaat dieper in op de indeling en opbouw van IP-adresreeksen. In deel III van het handboek staat hoe u IP-adressen kunt toekennen aan uw computers.

31.1 Basisbegrippen IP-reeks

Om met internet en kennisnet te communiceren, moet elke computer een uniek adres hebben, een IP-adres. Deze adressen zijn opgebouwd volgens het stramien '`a.b.c.d`', waarbij a t/m d getallen zijn van 0 tot 255. Een voorbeeld van zo'n IP-adres is `192.87.13.88`. Voor een netwerk zijn meerdere IP-adressen nodig, omdat elke computer in het netwerk een IP-adres nodig heeft. Zo'n reeks van IP-adressen is een IP-adresreeks.

Het netwerkadres is altijd het laagste adres in een IP-reeks. Het netwerkadres is *niet* bruikbaar als IP-adres voor een computer. Het hoogste adres in een reeks is het zogenoemde 'broadcast address' (omroepadres). Dit adres is bedoeld om alle aanwezige computers in een netwerkreeks aan te spreken; dit is nuttig voor sommige protocollen. Om het aantal bruikbare adressen te weten, moet u dus altijd twee adressen aftrekken van het aantal IP-adressen in een reeks.

Voorbeeld bruikbare adressen in IP-reeks

Een IP-reeks met netwerkadres 10.123.45.0 en 128 adressen. Het 'broadcast address' is het hoogste adres uit de reeks: 10.123.45.127. Het eerste bruikbare adres om uit te delen aan een computer is dan 10.123.45.1 en het laatste is dan 10.123.45.126.

Figuur 253: Bruikbare adressen in IP-reeks

De grootte van een reeks IP-adressen wordt meestal aangeduid met een zogenoemd netwerkmasker ('net mask'). Dit ziet eruit als een IP-adres, maar geeft aan hoeveel bits in het adres relevant zijn voor de desbetreffende reeks IP-adressen. Ieder stukje uit een IP-adres of een netwerkmasker is een getal van 0 tot 255, waardoor ieder stukje binair in exact acht bits kan worden gerepresenteerd.

31.2 Binaire berekening netwerkadres

Met het uitvoeren van een binaire 'AND'-operatie van het netwerkmasker op een willekeurig adres uit de reeks, wordt het netwerkadres verkregen. De binaire AND-operatie houdt in dat alle bits één voor één met elkaar worden vermenigvuldigd: overal waar in het netwerkmasker een '1' staat, blijft het bit op dezelfde positie in het adres ongewijzigd; waar een '0' staat, wordt het bit op dezelfde positie in het adres ook een '0'.

Met deze AND-operatie definieert u een 'subnet'. Een subnet is een gedeelte van een groter netwerk, bestaande uit een groter aantal IP-adressen.

Voorbeeld: AND-operatie voor subnet

In het eerder gegeven voorbeeld is het netwerkmasker 255.255.255.128. De binaire representatie hiervan is `11111111.11111111.11111111.10000000`. Een adres uit de reeks is bijvoorbeeld 10.123.45.67. Dit kan binair worden gerepresenteerd als `00001010.01111011.00101101.01000011`. Als u de AND-operatie uitvoert, krijgt u de volgende uitkomst:

IP-adres	`010.123.045.067`	`00001010.01111011.00101101.01000011`
Net Mask	`255.255.255.128`	`11111111.11111111.11111111.10000000`
Netwerkadres	`010.123.045.000`	`00001010.01111011.00101101.00000000`

Figuur 254: AND-operatie voor subnet

Een netwerkmasker wordt ook wel aangegeven met een schuine streep, gevolgd door een getal. Het getal geeft het aantal 'enen' in het netwerkmasker aan (de enen zijn altijd aaneengesloten). Zo kan het hierboven genoemde masker ook worden aangeduid als een '/25' (uitgesproken als '*slash vijfentwintig*').

31.3 Indeling IP-reeks (school)netwerk

31.3.1 IP-reeksen en netwerkmaskers

De IP-reeks van uw schoolnetwerk wordt ingedeeld in de volgende stukken:

- de router;
- één gereserveerd adres;
- werkplekken;
- lokale servers die op kennisnet 'zichtbaar' moeten zijn;
- lokale servers die *niet* op kennisnet 'zichtbaar' moeten zijn en overige netwerkapparatuur (hubs, routers, switches).

De indeling van de IP-adressen is voor *alle* kabelmaatschappijen en Energis gestandaardiseerd.

In netwerken met 32 of 64 adressen (netwerkmasker 255.255.255.224 of 255.255.255.192) wordt 3/4 (min de router, min een gereserveerd adres) van de adressen gebruikt voor werkplekken, 1/8 is bestemd voor servers die zichtbaar moeten zijn op kennisnet, en 1/8 voor afgeschermde servers.

Voor netwerken met 128 of meer adressen wordt 7/8 van de adressen (min de router, min een gereserveerd adres) gebruikt voor werkplekken, 1/16 is bestemd voor servers die zichtbaar moeten zijn op kennisnet, en 1/16 voor afgeschermde servers.

Er volgt nu een aantal voorbeelden van IP-reeksen en netwerkmaskers.

Let op!

Dit zijn fictieve adressen.

Voorbeeld (netwerkmasker: 255.255.252.0)

Netwerkadres: 212.180.0.0, netwerkmasker: 255.255.252.0, router: 212.180.0.1, gereserveerd adres: 212.180.0.2, start DHCP: 212.180.2.3, start servers zichtbaar: 212.180.3.128, servers niet zichtbaar: 212.180.3.192.

Voorbeeld (netwerkmasker: 255.255.254.0)

Netwerkadres: 212.180.0.0, netwerkmasker: 255.255.254.0, router: 212.180.0.1, gereserveerd adres: 212.180.0.2, start DHCP: 212.180.0.3, start servers zichtbaar: 212.180.1.192, servers niet zichtbaar: 212.180.1.224.

Voorbeeld (netwerkmasker: 255.255.255.0)

Netwerkadres: 212.180.0.0, netwerkmasker: 255.255.255.0, router: 212.180.0.1, gereserveerd adres: 212.180.0.2, start DHCP: 212.180.0.3, start servers zichtbaar: 212.180.0.224, servers niet zichtbaar: 212.180.0.240.

Voorbeeld (netwerkmasker: 255.255.255.128)

Netwerkadres: 212.180.0.0, netwerkmasker: 255.255.255.128, router: 212.180.0.1, gereserveerd adres: 212.180.0.2, start DHCP: 212.180.0.3, start servers zichtbaar: 212.180.0.112, servers niet zichtbaar: 212.180.0.120.

Voorbeeld (netwerkmasker: 255.255.255.192)

Netwerkadres: 212.180.0.0, netwerkmasker: 255.255.255.192, router: 212.180.0.1, gereserveerd adres: 212.180.0.2, start DHCP: 212.180.0.3, start servers zichtbaar: 212.180.0.48, servers niet zichtbaar: 212.180.0.56.

Voorbeeld (netwerkmasker: 255.255.255.224) Netwerkadres: 212.180.0.0, netwerkmasker: 255.255.255.224, router: 212.180.0.1, gereserveerd adres: 212.180.0.2, start DHCP: 212.180.0.3, start servers zichtbaar: 212.180.0.24, servers niet zichtbaar: 212.180.0.28.

Figuur 255: IP-reeksen en netwerkmaskers

31.3.2 Rekenhulpmiddel

Op http://beheer.kennisnet.nl/ vindt u een webpagina die u kunt gebruiken om de voor u toepasselijke IP-gegevens te berekenen. U moet hiervoor één IP-adres en het netwerkmasker bij de hand hebben. Als het goed is, heeft u deze van nl.tree ontvangen bij de aansluiting of, in het geval van voorhoedescholen, bij de IP-migratie[25].

31.4 Publieke en private IP-nummers

Zoals gezegd bestaat een IP-adres uit vier getallen van 0 tot en met 255. Hiermee kunnen in theorie 256*256*256*256=4.294.967.296 (ruim 4 miljard) adressen worden gevormd. Dit lijkt heel veel, maar aangezien lang niet alle adressen worden gebruikt en er inefficiënt wordt omgegaan met IP-adressen, is dit aantal toch onvoldoende.

In een bepaald document (ook wel bekend als RFC1597) is voorgesteld om een aantal reeksen IP-adressen te reserveren voor 'interne' netwerken die niet of niet rechtstreeks zijn verbonden met het internet: 'private internets'. De desbetreffende IP-adressen zijn ook wel bekend als 'private adressen' of 'private adresruimte' (Engels: 'private address space'). Deze private adresruimte omvat de volgende IP-reeksen:

- 10.0.0.0 t/m 10.255.255.255;
- 172.16.0.0 t/m 172.31.255.255;
- 192.168.0.0 t/m 192.168.255.255.

Private adressen kunnen niet op het internet worden gebruikt, de zogenoemde publieke adressen wel. Als een privaat netwerk wordt gekoppeld aan het internet, moeten de private adressen worden afgeschermd ('maskeren' of onzichtbaar maken). Door dit afschermen is niet mogelijk om alle internetdiensten door te laten. Daarom gebruikt kennisnet publieke IP-adressen.

31.5 Documentatie over IP en IP-adressen

Er is veel informatie beschikbaar over de werking van IP-netwerken. In de betere boekhandel zijn diverse boeken te vinden over protocollen en applicaties. Deze documentatie is meestal in het Engels.

Ook op het internet is veel informatie beschikbaar. Een goed en leesbaar document kunt u vinden op de website van 3Com, onder de titel 'Understanding IP Addressing':

http://www.3com.com/nsc/501302.html.

Als u zeer technische en gedetailleerde informatie wilt, kunt u de zogenoemde RFC- en STD-documenten raadplegen. Dit zijn documenten waarin standaarden worden voorgesteld voor het internet. Deze documenten zijn onder andere te verkrijgen via FTP op ftp://ftp.ripe.net/rfc/, respectievelijk ftp://ftp.ripe.net/std/.

[25] In de proeffase van kennisnet heeft er een omnummeroperatie plaatsgevonden m.b.t. de IP-adressen op kennisnet.

Handboek
Aansluiting van het schoolnetwerk op kennisnet

Deel VIII: Begrippenlijst, Afkortingenlijst, Figurenlijst en Index

32. Begrippenlijst

Dit hoofdstuk omvat een lijst met begrippen die met het internet en kennisnet te maken hebben. Bij elk van deze begrippen volgt een korte uitleg.

Apple	Een fabrikant van computersystemen. Zie ook Macintosh.
Bastion Host	Een bastion host is een speciale router en/of gateway die ervoor zorgt dat ongewenst netwerkverkeer niet van of naar het eigen netwerk kan. Hiermee kan (tot op zekere hoogte) worden voorkomen dat er oneigenlijk gebruik wordt gemaakt van machines binnen het eigen netwerk door gebruikers van buiten het eigen netwerk. Vaak wordt een bastion host aangeduid als een 'firewall'.
BOOTP	BOOTP staat voor Bootstrap Protocol. De primaire toepassing van dit protocol was om een – vaak diskloos – werkstation van de juiste software en/of gegevens te voorzien om op te starten en in het netwerk mee te laten functioneren. BOOTP wordt, met de opkomst van opvolger DHCP, niet erg veel meer als specifieke dienst gebruikt. kennisnet ondersteunt dit ook niet, maar indien noodzakelijk is het mogelijk om een eigen systeem op te zetten.
DHCP	Dynamic Host Configuration Protocol. Dit protocol maakt het mogelijk om alle adresgegevens die een computer nodig heeft om verbinding te maken met kennisnet, centraal uit te delen.
Discussiegroepen	Zie 'News'
DMZ	DeMilitarized Zone. Zie 'Gedemilitariseerde zone'
DNS	Domain Name Service. Dit kan het beste worden vergeleken met een soort telefoonboek of adressengids. Een DNS-server is in staat om een koppeling te maken tussen een machinenaam (bijvoorbeeld 'www.kennisnet.nl') en een IP-adres (bijvoorbeeld '195.61.115.2').
E-mail	E-mail is een afkorting van 'electronic mail' ofwel elektronische post. E-mail is te vergelijken met een brief of faxbericht. E-mail is één van de belangrijkste toepassingen van het internet, zo niet dé belangrijkste.
Ethernet	Een standaard waarmee computers op een lokaal netwerk kunnen communiceren. Boven op Ethernet kan bijvoorbeeld IP worden gebruikt om de machines onderling te adresseren.
Firewall	Een firewall is een verzameling van systemen die zorgen dat een intern netwerk wordt beveiligd tegen gevaren vanuit de buitenwereld. Tot een firewall worden gerekend: • een bastion host; • proxy-servers; • een gedemilitariseerde zone (DMZ). Vaak wordt het woord 'firewall' gebruikt om een bastion host aan te duiden. Soms is dit inderdaad het enige onderdeel van de beveiliging.
FTP	File Transfer Protocol. Met dit protocol kunnen bestanden worden uitgewisseld tussen computers. Het protocol voorziet ook in een vertaaloptie van ASCII-tekstformaten tussen verschillende computerplatformen.
Gateway	Een gateway is een onderdeel van een netwerk dat toegang biedt tot een ander netwerk. Een gateway vertaalt veelal de verzonden informatie en adressen, zodat het andere netwerk deze ook begrijpt.

Gedemilitariseerde zone	Een gedemilitariseerde zone (ook: DMZ) is een deel van het netwerk, dat systemen omvat die rechtstreeks kunnen communiceren met de buitenwereld. Deze systemen vormen vaak een tussenstap voor de communicatie tussen het interne netwerk en de buitenwereld.
HTTP	HyperText Transfer Protocol, het protocol waarmee webpagina's op het wereldwijde web worden verzonden van de aanbieder naar de lokale computer. Zie ook 'WWW'.
IMAP4	Interactive Mail Access Protocol, versie 4. Via dit protocol kan een e-mailprogramma berichten ophalen en terugplaatsen in een centrale e-mailopslag. Het protocol biedt goede mogelijkheden om e-mail centraal op te slaan en op een willekeurige plaats opnieuw te raadplegen.
Internet	Het internet is een groot netwerk dat op zich weer onderverdeeld is in kleinere netwerken die onderling gekoppeld zijn. Het internet is ooit ontstaan als een Amerikaans defensienetwerk (ARPANET). Later zijn ook educatieve en overheidsinstellingen aangesloten, en vervolgens andere netwerken in tientallen andere landen.
Intranet	Een intranet is een gesloten lokaal of bedrijfsnetwerk dat is gebaseerd op dezelfde technologie als die van het internet.
IP	Internet Protocol. Dit protocol zorgt ervoor dat gegevens over een netwerk van de ene machine naar de andere machine getransporteerd kunnen worden op basis van een afzender- en een ontvangeradres. Bovenop IP worden onder andere de protocollen TCP en UDP gedragen, die voor het transport en virtuele verbindingen zorg dragen.
IRC	Internet Relay Chat. IRC is een manier om met vele mensen tegelijk te kunnen 'chatten' (babbelen). Alle communicatie wordt via een centrale server geleid.
Kennisnet	Kennisnet is een landelijk, educatief computernetwerk, bedoeld om onder andere alle basis- en middelbare scholen alsmede instellingen voor agrarisch onderwijs en beroeps- en volwasseneneducatie met elkaar te verbinden.
LDAP	Lightweight Directory Access Protocol. Dit is een protocol om een soort adresboek ('directory') te raadplegen en te bewerken. In deze 'directory' bevinden zich de gegevens van alle gebruikers van kennisnet, waaronder hun gebruikersnamen, e-mailadressen en wachtwoorden.
Macintosh	Veelal afgekort als 'de Mac'. De Macintosh is een computersysteem van de fabrikant Apple. De Mac was de eerste, op grote schaal verkochte computer met een gebruikersvriendelijke grafische omgeving.
Masquerading	Een speciale vorm van NAT (zie 'NAT'). Masquerading is ook wel bekend als n:1-NAT. In het geval van masquerading worden alle IP-adressen aan de binnenkant van het lokale netwerk vertaald naar één IP-adres aan de buitenkant van het lokale netwerk, en omgekeerd voor terugwegverkeer.
NAT	Network Address Translation. Dit is een techniek die het mogelijk maakt om IP-adressen op een lokaal netwerk zó te vertalen, dat deze bruikbaar zijn op het internet en ook verkeer terug mogelijk is.
News	News, of ook 'Usenet News', is een systeem om middels een soort e-mailberichten met vele mensen tegelijk te kunnen discussieren over diverse onderwerpen. Er zijn op het internet duizenden verschillende 'discussiegroepen'. Daarnaast hebben sommige gesloten netwerken ook lokale discussiegroepen, zoals ook voor kennisnet het geval is.
NNTP	Network News Transfer Protocol. Dit is het protocol waarmee nieuwsberichten (zie 'News') worden uitgewisseld.

NTP	Network Time Protocol. Dit protocol wordt gebruikt voor een nauwkeurige tijdsynchronisatie. Dit protocol houdt onder andere rekening met de afstand tussen servers (lees: de tijd die een pakket nodig heeft om van de ene machine naar de andere te komen) en referentieservers. Kennisnet biedt ook NTP om servers en werkstations te synchroniseren. Deze systemen zijn bereikbaar als '`time.kennisnet.nl`'.
POP3	PostOffice Protocol, versie 3. Dit protocol kan gebruikt worden om met een e-mailprogramma e-mail op te halen vanaf een mailserver. Het protocol is redelijk rechttoe rechtaan en biedt weinig extra mogelijkheden.
Proxy	De vertaling van het Engelse woord 'proxy' is 'gevolmachtigde' of 'vertegenwoordiger'. Dit geeft ook redelijk aan wat een proxy doet: uit naam of op verzoek van de gebruiker haalt het gegevens op van, of legt het verbindingen met andere computers, veelal buiten het lokale netwerk van de gebruiker.
RFC	Een RFC (Request For Comments) is een document dat belangrijke informatie over internetprotocollen, gebruiken of gedragsregels bevat. In RFC's worden standaarden en mogelijke aanstaande standaarden alsmede revisies hiervan beschreven. Voordat een protocol tot standaard wordt verheven, is er echter een lange weg afgelegd. De RFC-documenten kunt u onder andere vinden op het adres ftp://ftp.ripe.net/rfc/.
RJ45	Een specificatie voor een type aansluiting (stekkertje en contactje).
Router	Een router is een soort computer die zich uitsluitend bezighoudt met het in goede banen leiden van het netwerkverkeer. Als een pakketje aan de router wordt aangeboden met een bestemmingsadres, dan zal deze proberen het pakketje op een dusdanige manier door te sturen, dat het uiteindelijk op de juiste bestemming terecht zal komen.
RTSP	Real Time Streaming Protocol. Dit is een protocol om beelden en geluiden in een ononderbroken stroom over het internet te verzenden. Via dit protocol kunnen bijvoorbeeld radio-uitzendingen of tv-programma's via het intemet worden gevolgd, of korte filmpjes worden bekeken.
Serverpark	Het serverpark is een verzameling van grote computersystemen ('servers') die elk bepaalde diensten verzorgen voor kennisnet.
SMTP	Simple Mail Transfer Protocol. Dit protocol wordt gebruikt om e-mail op het internet te verzenden van een e-mailprogramma naar een server, en tussen servers onderling.
SNTP	Simple Network Time Protocol. Dit protocol is een vereenvoudigde versie van NTP. SNTP biedt nog steeds een nauwkeurige manier om de tijd tussen twee systemen te synchroniseren, maar vereist iets minder zekerheden dan NTP. Zie 'NTP'.
TCP	Transmission Control Protocol. Dit protocol draagt zorg voor het opzetten van een (virtuele) verbinding tussen twee eindpunten en het, opgedeeld in pakketjes, verzenden van informatie. TCP garandeert dat de informatie aankomt en wel in de juiste volgorde. TCP vereist IP (het internet Protocol) om te kunnen functioneren. IP zorgt voor de adressering, terwijl TCP voor een virtuele verbinding zorgt.
'Trojaans Paard' of 'Trojan Horse'	Een 'Trojaans Paard' is een programma dat, terwijl het wordt gebruikt, andere programmatuur op de computer probeert te besmetten met een computervirus. De naam is afkomstig van de oude Griekse legende van de overwinning op de stad Troje, waarbij de aanvallende Grieken deden of zij zich gewonnen gaven en 'als geschenk' aan de stad Troje een houten paard achterlieten. In werkelijkheid zaten er soldaten in het houten paard, die 's nachts uit het door de Trojanen binnengehaalde paard klommen en de stad van binnenuit aanvielen.

UDP	User Datagram Protocol. Dit protocol kan pakketjes informatie verzenden van één computer naar één of meer andere computers op een netwerk. In vergelijking met TCP heeft UDP minder mogelijkheden om fouten te herstellen en is de aankomst van de informatie niet gegarandeerd.
UNIX	UNIX is een merknaam van een besturingssysteem voor van origine grote computersystemen. Deze naam wordt echter ook gebruikt als verzamelnaam voor een complete familie van besturingssystemen die op hetzelfde idee zijn gebaseerd. Er zijn tegenwoordig ook uitvoeringen van dit besturingssysteem, die prima functioneren op gangbare computersystemen zoals PC's.
Virus	Een virus is programmatuur die speciaal is gemaakt om zich te kopiëren en zichzelf verder te verspreiden. Veel virussen zijn bovendien zo geprogrammeerd dat ze ook schade aanrichten onder bepaalde omstandigheden, na enige tijd op het systeem te hebben bestaan of op vaste tijdstippen ('vrijdag de dertiende' en dergelijke).
Web	Zie 'WWW'.
Windows	Microsoft Windows is een grafische omgeving voor computers, waarmee men in staat wordt gesteld om speciale grafische programmatuur te gebruiken.
WWW	World Wide Web. Een systeem van wereldwijd verspreide informatie die op basis van 'hyperlinks' (verwijzingen) met elkaar is gekoppeld. Door de verwijzingen te selecteren, kunt u van de ene pagina met informatie naar de andere pagina surfen. De informatie kan bestaan uit opgemaakte teksten, afbeeldingen, beeld- en geluidsfragmenten.

33. Afkortingenlijst

A

ACL........Access Control Lists
AUI........Attachment Unit Interface

B

BIND........Berkeley Internet Name Domain
BNC........Bayonet Navy Connector
BOOTP........Bootstrap Protocol
BRIN........BasisRegistratie INstellingen

C

CARP........Caching Array Routing Protocol
CGI........Common Gateway Interface
CSV........Comma Seperated Values

D

DHCP........Dynamic Host Configuration Protocol
DMZ........Demilitarized Zone
DNS........Domain Name Service

F

FTP........File Transfer Protocol

G

GnuPG........GNU Privacy Guard

H

HTML........HyperText Markup Language
HTTP........HyperText Transfer Protocol

I

ICP........Internet Caching Protocol
ICT........Informatie - en Communicatietechnologie
IDNL........Stichting Internet Domeinregistratie Nederland
IMAP........Interactive Mail Access Protocol
IP........Internet Protocol
IRC........Internet Relay Chat
ISC........The Internet Software Consortium
ISP........Internet Service Provider

K

kb/s........Kilobits per seconde
kB/s........Kilobytes per seconde

L

LAN........Local Area Network
LDAP........Lightweight Directory Access Protocol
LED........Light Emitting Diode

M

Mb/s........Megabits per seconde
MB/s........Megabytes per seconde

MIME.......Multipurpose Internet Mail Extensions

N

NAT.......Network Address Translation
NetBIOS.......Network Basic Input/Output System
NNTP.......Network News Transfer Protocol

O

OOP.......Onderwijsondersteunend Personeel

P

PDF.......Portable Document Format
PGP.......Pretty Good Privacy
POP.......PostOffice Protocol
PPP.......Point-to-Point Protocol

R

RFC.......Request For Comments
RTB.......Regionaal Telecommunicatie Bedrijf
RTSP.......Real Time Streaming Protocol

S

SMTP.......Simple Mail Transfer Protocol
SNTP.......Simple Network Time Protocol
SPK.......Servicepunt Kennisnet
SSH.......Secure Shell
SSL.......Secure Sockets Layer

T

TCP.......Transmission Control Protocol
TTL.......Time To Live

U

UTP.......Unshielded Twisted Pair

V

VPN.......Vitual Private Network

W

WINS.......Windows Internet Naming Service

34. Figurenlijst

35. Index

N

O

P

Handboek
Aansluiting van het schoolnetwerk op kennisnet

Aanvullingen

Handboek
Aansluiting van het schoolnetwerk op kennisnet

Persoonlijke aantekeningen